抽象代数讲义

黎永锦 编著

科学出版社

(O—4704.0101)

www.sciencep.com

ISBN 978-7-03-033935-5

科学出版中心 数理分社
电 话：(010) 64033664
E-mail：math-phy@mail.sciencep.com
网 站：http://www.math-phy.cn

销售分类建议：高等数学

定 价：58.00 元

抽象代数讲义

黎永锦　编著

科学出版社

北京

内 容 简 介

本书是根据作者近年来在中山大学数学系讲授抽象代数课程的讲义写成的. 全书共 7 章. 第 1 章群论, 第 2 章环和域, 第 3 章环上的多项式, 第 4 章向量空间, 第 5 章 Sylow 定理和可解群, 第 6 章域的扩张, 第 7 章群论在微分方程中的应用. 书中附有习题和部分解答. 本书的特点是加强了代数与分析的联系, 书中还介绍了代数的一些较新的结果.

本书可作为高等院校数学专业高年级本科生和研究生学习抽象代数的教材, 也可供相关专业教师阅读参考.

图书在版编目(CIP)数据

抽象代数讲义/黎永锦编著. —北京：科学出版社, 2012
ISBN 978-7-03-033935-5
Ⅰ. ①抽… Ⅱ. ①黎… Ⅲ. ①抽象代数－高等学校－教材 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2012) 第 054850 号

责任编辑: 李 欣 赵彦超／责任校对: 李 影
责任印制: 钱玉芬／封面设计: 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销
*
2012 年 5 月第 一 版 开本: B5(720×1000)
2012 年 5 月第一次印刷 印张: 15 1/4
字数: 290 000

定价: 58.00 元

(如有印装质量问题, 我社负责调换)

前　言

抽象代数是现代数学中的重要分支之一, 它产生于 19 世纪, 是研究各种抽象的公理化代数系统的数学学科. 抽象代数包含群、环、域和伽罗瓦理论等许多分支, 并与数学其他分支相结合产生了代数几何、代数数论、代数拓扑、拓扑群等数学学科. 通过这一课程, 学生可了解抽象代数的基本思想、原理及在其他学科中的应用, 掌握抽象代数的基本概念和重要的定理, 学会用代数处理问题的方法, 还可以加深学生理解数学理论的基本思想, 提高抽象思维能力. 抽象代数为学习代数几何、代数数论、代数拓扑、Banach 代数、李群等课程打下基础. 另外, 抽象代数的主要内容群、环、域等与物理学、化学等有紧密的联系, 总之, 它不仅在数学的各个分支有广泛的应用, 而且在许多现代科学, 如量子力学、结晶学、理论物理、量子化学以及密码学、系统科学、数理经济等领域都有广泛的应用.

本书根据作者在中山大学数学系讲授抽象代数课程时的讲稿, 在多年的教学过程中不断修改而成. 书中尽可能地介绍抽象代数中一些概念和定理的来历, 让学生可以了解一些抽象代数的历史, 提高学习兴趣. 不需要具有点集拓扑学的知识, 只要有数学分析和高等代数中关于矩阵和多项式的基础, 阅读本书是不会有困难的. 本书刻意加强了抽象代数和数学分析的连接, 目的是使抽象代数更加接近数学分析. 本书内容共分 7 章. 第 1 章是群论, 为了加强与点集拓扑学的联系, 编写了拓扑群一节, 简单地对拓扑群作了介绍. 在第 2 章中环上的微分和拓扑环部分, 加强了环与分析和拓扑的连接. 第 3 章环上的多项式中的非交换环上的多项式这一节, 给出了多项式在环不交换的情况下的特殊性质. 考虑到较多的抽象代数教材讲述的内容与数学其他学科的交叉很少, 因此编写了第 7 章, 目的是让学生初步理解抽象的群论等在微分方程等其他数学分支有着广泛的应用. 在教学时, 拓扑群和拓扑环以及群论在微分方程中的应用可以不讲或选讲. 本书可作为抽象代数的一本入门教材, 书中选有一定的习题. 书中的习题参考了很多抽象代数习题解答的书, 如腾加俊的《近世代数辅导与习题精解》、冯克勤的《近世代数三百题》等, 有些习题修改后比较难说明其出处, 无法指出并一一致谢. 为了教学的方便, 双数序号的习题都有解答, 单数序号的习题一般不再给出答案.

书中数学家的头像等图片是作者自己用电脑制作的, Galois 的图像是我的学生

张余的作品. 我要向我的学生们表示衷心的感谢, 龙永彪、王俊涛、邹昆儒、黄栋超、庄跃鸿、王观发等对本书的改进和校对做了很多的工作. 刘佩、赵志红、和炳和顾朝晖等在校对时提出了很多很好的意见. 在多年来的教学过程中, 我从学生身上学到了很多东西, 本书正是在他们的帮助下不断修改完善的结果.

黎永锦

2011 年 8 月于中山大学

符 号 表

$\mathbf{Q}$	有理数域
$\mathbf{R}$	实数域
$\mathbf{C}$	复数域
$\mathbf{Z}$	整数集合, 正负整数, 包含 0
$\mathbf{N}$	自然数集
$a\|b$	a 整除 b
$a \equiv b(\mathrm{mod}m)$	a 与 b 模 m 同余
(a,b)	a 和 b 的最大公因子
$o(a)$	a 的阶
$\|G\|$	群 G 的阶
S_n	n 个字母的对称群
$\mathbf{Z}_n$	模 n 整数加法群或环
$\mathbf{Z}_p$	模 p 整数加法群或域 (p 为素数)
$\cong$	同构
$\mathrm{Ker}(f)$	同态 f 的核
$< H >$	由集合 H 生成的子群
$< a >$	由元素 a 生成的循环子群
aH, Ha	a 的左陪集和右陪集
$[G:H]$	子群 H 在群 G 中的指数
GH	$\{ab\|a \in G, b \in H\}$
$H \triangleleft G$	H 为 G 的正规子群
G/H	G 对 H 的商群
$\mathrm{sgn}\sigma$	置换 σ 的符号
A_n	n 个字母的交错群
$C_H(a)$	a 在 H 中的中心化子
$N_H(K)$	H 在 K 中的正规化子
$C(G)$	G 的中心
G'	G 的换位子群
$G^{(n)}$	G 的第 n 次导群

$\mathrm{char}R$	环 R 的特征
(H)	由集合 H 生成的理想
(a)	由元素 a 生成的主理想
$F[x]$	F 上的多项式环
$F[x_1, x_2, \cdots, x_n]$	F 上 n 个未定元的多项式环
$\deg f$	多项式 f 的次数
$\dim V$	线性空间 V 的维数
G_f	多项式 f 的伽罗瓦群
H^{-1}	$H^{-1} = \{a^{-1} \mid a \in H\}$
$R[a]$	由 R 和 a 生成的环, 包含 R 和 a 的最小环
$F(a)$	域 F 上的单扩张
$[K : F]$	域扩张 K/F 的次数

我们是孩子, 但我们精力充沛,
勇往直前…
——伽罗瓦(E. Galois, 1811—1832)

目　　录

前言
符号表
第 1 章　群论……1
1.1　群的定义……1
1.2　子群……5
1.3　置换群……10
1.4　陪集……16
1.5　正规子群……22
1.6　交错群……29
1.7　群的同态……31
1.8　群的直积……37
1.9　拓扑群……41
习题一……44
学习指导……47
第 2 章　环和域……52
2.1　基本概念……53
2.2　理想和商环……59
2.3　环的同态……65
2.4　域……69
2.5　环上的微分……75
2.6　拓扑环……77
习题二……80
学习指导……83
第 3 章　环上的多项式……88
3.1　多项式……88
3.2　带余除法……92
3.3　因式分解……100
3.4　本原多项式……108
3.5　唯一因子分解环上的多项式……111
3.6　非交换环上的多项式……113

习题三 ····· 118
学习指导 ····· 120
第 4 章　向量空间 ····· 125
4.1　向量空间 ····· 125
4.2　内积空间 ····· 131
4.3　模 ····· 134
习题四 ····· 139
学习指导 ····· 141
第 5 章　Sylow 定理和可解群 ····· 144
5.1　群作用 ····· 144
5.2　Sylow 定理 ····· 151
5.3　可解群 ····· 156
习题五 ····· 163
学习指导 ····· 165
第 6 章　域的扩张 ····· 168
6.1　子域和扩域 ····· 168
6.2　代数扩张 ····· 173
6.3　Galois 域和分裂域 ····· 178
6.4　方程的根式解 ····· 189
习题六 ····· 196
学习指导 ····· 198
第 7 章　群论在微分方程中的应用 ····· 202
7.1　微分方程的不变群 ····· 202
7.2　一阶常微分方程的求解 ····· 207
7.3　常微分方程的降阶 ····· 210
习题七 ····· 211
学习指导 ····· 212
参考文献 ····· 214
部分习题解答 ····· 215
索引 ····· 231

第1章 群 论

最有价值的科学书籍是作者在书中明白地指出了他所不明白的东西的那些书, 遗憾地, 这还很少被人们所认识; 作者由于掩盖难点, 大多害了他的读者.

伽罗瓦 (1811—1832, 法国数学家)

群论起源于解高次方程, 它的思想可以追溯到 Lagrange. Lagrange 关于方程式根的对称函数的工作, 使人们注意到根的置换的性质, 从而导致置换群理论的产生. 18 世纪末, Lagrange, Vandermonde, Ruffini 等试图求出高次代数方程的代数解法, 由研究方程诸根之间的置换而注意到了群的概念, 挪威数学家 Abel 证明了 5 次以上的一般的代数方程没有根式解. 而置换群与代数方程之间的关系的完全描述是由伽罗瓦在 1830 年左右做出的, Jordan 在《置换和代数方程论》中对伽罗瓦理论作了很好的介绍. 很多数学家都对群论的发展做出了巨大贡献, 如 Möbius, Cayley, Klein 等. 群的概念已经被认为是数学及其应用中最基本的概念之一, 在几何学、代数拓扑学、泛函分析等学科中起着重要的作用, 并形成了拓扑群、李群、代数群等新学科. 同时, 群论在理论物理、量子化学以及编码学等都有重要的应用.

1.1 群的定义

群论对 19~20 世纪的数学整体发展影响深远, 群论的影响不仅深入数学领域的每个分支, 还在某种程度上促进了数学各个分支的统一.

1 二元运算

定义 1.1.1 设 S 和 G 都是集合, 则称所有有序对 (a,b) 构成的集合为它们的笛卡儿积, 其中 $a\in S$, $b\in G$, 记为 $S\times G$.

在算术中, 若 a, b 都是整数, 则 a 和 b 的加法运算将 a 和 b 从整数集 $\mathbf{Z}\times\mathbf{Z}$ 映

到 $\mathbf{Z}$. 类似地, 在集合上, 可以定义二元运算.

定义 1.1.2　从 $S\times S$ 到 S 的一个映射 $\cdot$ 称为 S 上的一个二元运算.

也就是说, 对 S 中的任何一对元素 (a,b) 都有 S 中唯一确定的一个元素 $a\cdot b$ 与之对应.

例 1.1.1　取 S 为实数全体所构成的集合, 将映射 $\cdot$

$$\cdot : S\times S\to S$$

定义为

$$a\cdot b=a^2+b^2,$$

则 $\cdot$ 就是一个二元运算.

例 1.1.2　设 $S=\{(a_1,a_2)|a_1,a_2$ 都是实数$\}$是二维欧氏空间, 则向量和 $u+v$, 矢量积 $u\times v$ 都是二元运算. 但内积的结果不再是向量, 而是一个数, 因此内积不是二元运算.

例 1.1.3　设 S 是 n 阶方阵全体所构成的集合, 则 $A+B$, AB, $AB-BA$ 是三种不同的二元运算.

2　群的定义和例子

伽罗瓦, Jordan 和 Klein 只用封闭性公理来定义群, 不过他们考虑的是置换或变换的有限群, 因此其他的公理都隐含在他们的论文里面. Cayley 在 1854 年的论文中才明确了群要有结合律和单位元. 1882 年 Dyck 和 Weber 都发表了完整的群的公理.

定义 1.1.3　设 G 是一个非空集合, 若在 G 上定义一个二元运算 $\cdot$, 满足

(1) 结合律: 对任何 $a,b,c\in G$, 有 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$, 则称 G 是一个半群 (semigroup), 记作 $(G,\cdot)$. 若 $(G,\cdot)$ 还满足

(2) 存在单位元 $e\in G$, 使对任何 $a\in G$ 有 $e\cdot a=a\cdot e=a$.

(3) 对任何 $a\in G$, 有 $a^{-1}\in G$, 使得 $a^{-1}\cdot a=a\cdot a^{-1}=e$, 则称 $(G,\cdot)$ 是一个群 (group).

如果半群中也有单位元, 则称为幺半群 (monoid).

幺半群不一定是群, 如整数集 $\mathbf{Z}$ 对于乘法是一个幺半群, 但它不是群.

如果群 $(G,\cdot)$ 适合交换律: 对任何 $a,b\in G$ 有 $a\cdot b=b\cdot a$, 则称 G 为交换群或 Abel **群.**

Abel 于 1827 年发现, 如果多项式方程的根的伽罗瓦群是交换的, 那么该多项式方程一定可以用公式求解, Abel 群这一术语是 Jordan 在 1872 年引入来纪念数学家 Abel 的. 对于 Abel 群, 群运算常常称为加法, 记为 $a+b$. 这时单位元称为零元, 记作 0, 元素 a 的逆元记作 $-a$. 对任意自然数 n, 元素 a 的 n 倍 na 定义为 n 个 a 相加.

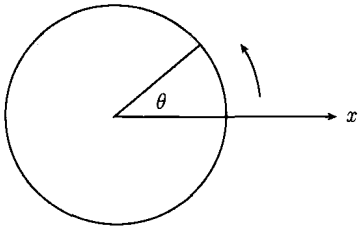
Niels Henrik Abel(1802—1829)

群中的乘法运算一般简记为 ab. **如果 $ab=ba=e$, 那么就称 a 为一个可逆元** (invertible element) **并称 b 为 a 的逆元** (inverse element). **可逆元 a 的逆元通常记作 a^{-1}. 容易知道可逆元的逆元是唯一的.**

例 1.1.4 整数集 $\mathbf{Z}$ 对普通加法构成 Abel 群.

例 1.1.5 实数集 $\mathbf{R}$ 对普通加法构成 Abel 群, 但在乘法下不是群.

例 1.1.6 $[0,1]$ 上的所有实连续函数 $C[0,1]$ 全体加法构成 Abel 群, 但在函数相乘的乘法下不是群.



例 1.1.7 所有 2×2 可逆矩阵 $GL(2,\mathbf{R})$ 全体在矩阵的相乘的乘法下构成非交换群, 其单位元就是单位矩阵.

例 1.1.8 对于 $0\leqslant\theta<2\pi$, 所有形如

$$\begin{bmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{bmatrix}$$

的矩阵, 在矩阵乘法下是一个群. 容易知道这是平面上的旋转.

例 1.1.9 设 $K_4=\{e,a,b,c\}$, 乘法表为

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

则 K_4 是一个交换群, 称为**克莱因四元群**(Klein four-group), 记作 $\{e,a,b,ab\}$, 它是 Klein 在 1884 年给出的.

上面例子中的表一般称为**群的乘法表**(multiplication table), 也称为**群表**(group table) 或**凯莱表**(Cayley table). 乘法表常用来表示有限群的运算. 群表是凯莱在 1854 年的论文 *On the theory of groups, as depending on the symbolic equation* $\theta^n=1$ 中首次提出的. 通过群表, 可以直观地了解该群的单位元及是否交换等.

3　群的性质

性质 1.1.1(消去律)　*设群 G 中的元素 a, b, c 满足 $ab=ac$ 或 $ba=ca$, 则 $b=c$.*

Felix Christian Klein(1849—1925)

证明　若 $ab=ac$, 则在等式两边同时左乘 a^{-1}, $a^{-1}(ab)=a^{-1}(ac)$, 由结合律可知

$$(a^{-1}a)b=(a^{-1}a)c,\ \text{故}\ eb=ec,\ \text{所以}\ b=c.$$

同理, $ba=ca$ 时, 有 $b=c$. ■

容易知道, 设 G 是群, 则对任意的 $a,b\in G$, 方程 $ax=b$ 和 $ya=b$ 在 G 中都有唯一解. 不难验证, 群还具有下面的一些简单性质.

性质 1.1.2　*设 a, b 是群 G 中的两个元素.*

(1) *若 $ab=a$ 或 $ba=a$, 则 $b=e$;*

(2) *若 $ab=e$ 或 $ba=e$, 则 $b=a^{-1}$;*

(3) $(a^{-1})^{-1}=a$;

(4) $(ab)^{-1}=b^{-1}a^{-1}$.

4　元素的阶

Cayley 在 1815 年定义了群的元素的阶.

定义 1.1.4　*由有限多个元素构成的群 G 称为有限群* (finite group), *其中元素的个数记作 $|G|$, 称为 G 的阶* (order). *用 $|G|=\infty$ 表示 G 是无限群.*

定义 1.1.5　若 a 是群 G 的一个元, 则使得 $a^n = e$ 的最小的正整数 n 称为 a 的阶或周期, 记为 $o(a)$. 若这样的正整数 n 不存在, 则称 a 的阶为无穷.

例 1.1.10　2×2 可逆矩阵 $GL(2, \mathbf{R})$ 群中, 由于矩阵

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad A^n = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix},$$

故 A 的阶是无穷.

定理 1.1.1　若 a 的阶为 m, 则 $a^n = e$ 当且仅当 m 整除 n.

证明　设 m 整除 n, 则存在整数 k, 使得 $n = mk$. 故

$$a^n = a^{mk} = e.$$

反过来, 若 $a^n = e$, 但 m 不整除 n, 则 $n = mk + r$, $1 \leqslant r < m$. 于是 $a^r = a^{mk+r} = a^n = e$, 但这与 m 是 a 的阶矛盾. ■

思考题 1.1.1　是否存在一个群, 除了单位元外, 所有的元的阶都是无穷?

例 1.1.11　所有非零正实数 G 在乘法下是一个群, 容易看出该群除了单位元外, 所有的元的阶都是无穷.

思考题 1.1.2　对任意自然数 n, 是否存在一个群 G, G 的阶就是 n?

例 1.1.12　设 C 为复数, 则所有 n 次单位根构成的集合

$$\begin{aligned} G &= \{a \in C | a^n = 1\} \\ &= \left\{ \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n} | k = 0, 1, 2, 3, \cdots, n-1 \right\} \end{aligned}$$

在乘法下, 就是一个 n 阶的 Abel 群.

1.2 子　群

如果群 G 的子集 H 对 G 的运算构成群, 那么称它是 G 的子群. 通过研究子群 H 的性质, 可以了解群 G 的一些整体性质.

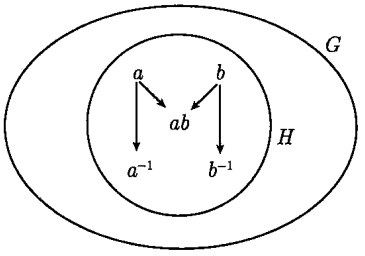
1　子群的定义

定义 1.2.1　设 H 是群 G 的满足下面两个条件的一个非空子集:

(1) (乘法封闭) 对 H 中的任意元 a 和 b 都有 $ab \in H$;

(2) (求逆封闭) 对 H 中的任意元 a 都有逆元 $a^{-1} \in H$.

则称 H 为 G 的一个子群.



根据乘法封闭性, H 中的乘法运算是有意义的. 乘法结合律自然成立. 由于 H 非空, 存在 $a \in H$. 于是 $a^{-1} \in H$, $e = a^{-1}a$. 因此 H 含有单位元. 所以 H 在乘法下构成一个群, 这就是"子群" 这个名词的意义.

容易看出, Abel 群的子群仍然是 Abel 群.

例 1.2.1　每个群 G 一定有两个子群 $\{e\}$ 和 G, 称为 G 的平凡子群.

例 1.2.2　设 n 是一个自然数, 令 $n\mathbf{Z}$ 为所有被 n 整除的整数所构成的集合, 它是整数加法群 $\mathbf{Z}$ 的子群.

例 1.2.3　令 $SL_n(K)$ 为数域 K 上行列式等于 1 的 n 阶方阵全体所构成的集合, 它是 n 阶可逆矩阵群 $GL_n(K)$ 的子群, 称为**特殊线性群**(special linear group).

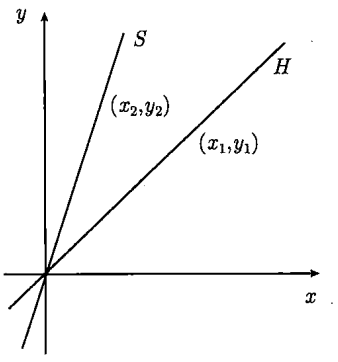
例 1.2.4　设 l_∞ 为所有有界实数列全体, 则在加法下它是一个群, 若 c_0 为所有收敛到零的实数列全体, 则在加法下 c_0 是 l_∞ 的一个子群.

在 $\mathbf{R}^2$ 按坐标的加法所构成的加法群中, 容易看出过点 (x_1, y_1) 的子群 H 在过点 (x_1, y_1) 和 $(0,0)$ 的直线内. 但经过点 (x_1, y_1) 的子群不是唯一的, 如

$$H_1 = \{(nx_1, ny_1) | n \text{ 为整数}\},$$

$$H_2 = \{(qx_1, qy_1) | q \text{ 为有理数}\}$$

都是 $\mathbf{R}^2$ 经过点 (x_1, y_1) 的子群. 另外, 经过点 (x_2, y_2) 和 $(0,0)$ 的直线一定是 $\mathbf{R}^2$ 的一个子群, 如右图中的 S 和 H 都是 $\mathbf{R}^2$ 的子群.



2 子群的性质

命题 1.2.1(子群判别法)　设 H 是群 G 的一个非空子集, 若 $ab^{-1} \in H$ 对任意 $a, b \in H$ 成立, 则 H 是 G 的一个子群.

证明　任取 $c \in H$, 则 $e = cc^{-1} \in H$. 对任意的 $a \in H$, 有 $a^{-1} = ea^{-1} \in H$, 因此 H 对求逆封闭. 对任意 $a, b \in H$ 都有 $ab = a(b^{-1})^{-1} \in H$, 故 H 对乘法封闭. 所以 H 是 G 的一个子群. ■

性质 1.2.1　设 $\{H_\alpha\}_{\alpha \in I}$ 是群 G 的任意多个子群, 则 $H = \cap_{\alpha \in I} H_\alpha$ 是 G 的一个子群.

证明　由于 $e \in \cap_{\alpha \in I} H_\alpha$, 故 H 非空. 设 $a, b \in H$, 则 $ab^{-1} \in H_\alpha$ 对每个 $\alpha \in I$ 成立, 故 $ab^{-1} \in H$, 所以 H 是 G 的一个子群. ■

3 中心化子

定义 1.2.2　设 g 是群 G 的一个元素, 则集合 $C(g) = \{a \in G | ag = ga\}$ 称为 g 在 G 中的中心化子 (centralizer), 设 $S \subseteq G$, 则集合 $C(S) = \{a \in G | ag = ga$ 对所有 g $\in S\}$ 称为 S 在 G 中的中心化子. $C(G)$ 称为 G 的中心 (center).

例 1.2.5　所有对角线上都是 1 的 3×3 实上三角矩阵 G 全体在矩阵的相乘的乘法下构成非交换群, G 的中心 $C(G)$ 就是形如:

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

的实矩阵全体构成的子群.

明显地, $C(g)$ 和 $C(S) = \cap_{g \in S} C(g)$ 都是 G 的子群. 容易看出, 下面性质成立.

性质 1.2.2　(1) G 的中心 $C(G)$ 是 Abel 群.

(2) G 是 Abel 群当且仅当 G 的中心 $C(G)$ 就是 G.

性质 1.2.3　设 H_1 和 H_2 是群 G 的子集, $H_1 \subseteq H_2$, 则

(1) $C(H_1) \supseteq C(H_2)$;

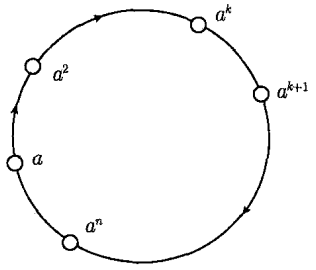
(2) $H_1 \subseteq C(C(H_1))$;

(3) $C(H_1) = C(C(C(H_1)))$.

4　由集合生成的子群

定义 1.2.3　设 S 为群 G 的一个子集, 令 $< S >$ 为所有包含 S 的子群的交, 那么 $< S >$ 为包含 S 的最小子群, 称为 S 生成的子群. 若 $G =< S >$, 则称 G 由 S 生成.

例 1.2.6　易知整数群 $\mathbf{Z}$ 可以由 1 或 -1 生成.



定义 1.2.4　若群 G 由一个有限子集生成, 则称 G 是有限生成的. 若 G 可以由一个元素 a 生成, 则称 G 为循环群 (cyclic group). 记为 $G =< a >$.

明显地, 任何一个循环群是 Abel 群.

设 $a \in G$, 则 $< a >$ 是 G 的一个子群, 它本身是一个循环群, 称 $< a >$ 为 G 的一个循环子群, 明显地 $o(a) = | < a > |$.

容易知道, 若 $o(a)=\infty$, 则 $< a >=\{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\}$. 若 $o(a)=n<\infty$, 则 $< a >= \{e, a, a^2, \cdots, a^{n-1}\}$.

例 1.2.7　在 n 阶可逆矩阵群 $GL_n(K)$ 中矩阵

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

生成一个无限阶子群, 矩阵

$$\begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

生成一个三阶循环子群.

思考题 1.2.1　若群 G 的所有子群都是循环群, 则 G 一定是循环群吗?

不一定. 如 $G = \{(0,0), (1,0), (1,1), (0,1)\}$ 在加法 $(a,b)+(c,d) = (a+c, b+d)$, 并且两个坐标都按 $0+1 = 1+0 = 1$, $1+1 = 0$ 来进行计算, 则 G 是加法群, 并且它的每个子群都是循环群, 但 G 不是循环群.

定理 1.2.1　设 S 是群 G 的一个子集, 则

$$< S >= \{a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n} | a_1, \cdots, a_n \in S, k_1, \cdots, k_n \in Z\}.$$

证明　记 $K = \{a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n} | a_1, \cdots, a_n \in S, k_1, \cdots, k_n \in Z\}$, 明显地, K 是包含 S 的一个子群, 因此 $< S >\subseteq K$.

反过来, 设 H 是包含 S 的一个子群, 由于子群 H 对乘法和求逆封闭, 故形如 $a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n}(a_i \in S, k_i \in \mathbf{Z})$ 的元素都在 H 中, 于是 $K \subseteq H$, 所以 $< S >= K$. ■

例 1.2.8　试找出整数加法群 $\mathbf{Z}$ 的所有子群.

证明　容易知道, $\{0\}, \mathbf{Z}, 2\mathbf{Z}, 3\mathbf{Z}, \cdots$ 都是 $\mathbf{Z}$ 的子群.

下面证明 $\mathbf{Z}$ 一定没有其他子群. 设 H 是 $\mathbf{Z}$ 的一个非平凡子群, 则它含有非零整数. 由于 H 对求逆封闭, 故 H 含有正整数. 设 n 是 H 中最小的正整数. 则 $n\mathbf{Z} \subseteq H$. 对任何 $m \in H$, 根据欧氏除法, 存在整数 q, r 使 $m = qn + r$, 其中 $0 \leqslant r < n$. 由于 $r = m - qn \in H$, 根据 n 的最小性推得 $r = 0$, 故 $m \in n\mathrm{Z}$, 从而 $H \subseteq n\mathrm{Z}$. 明显地, $n\mathrm{Z} \subseteq H$, 因而 $n\mathrm{Z} = H$, 所以 $\mathbf{Z}$ 一定没有其他子群.

5　子群的乘积

思考题 1.2.2　若 H_1 和 H_2 是群 G 的子群, 则 H_1H_2 一定是 G 的子群吗?

例 1.2.9　设 H_1 和 H_2 是群 G 的子群, 试证明 H_1H_2 是 G 的子群的充要条件为 $H_1H_2 = H_2H_1$.

证明　若 $H_1H_2 = H_2H_1$, 则容易验证 H_1H_2 对于乘法和求逆都封闭, 因此 H_1H_2 是 G 的子群.

反过来, 若 H_1H_2 是 G 的子群, 则对任意的 $a \in H_1, b \in H_2$, 有

$$ba = (eb)(ae) \in (H_1H_2)(H_1H_2) \subseteq H_1H_2,$$

从而 $H_2H_1 \subseteq H_1H_2$.

由于 $a \in H_1, b \in H_2$ 时, 据 H_1H_2 是 G 的子群可知 $(ab)^{-1} \in H_1H_2$, 故

$$ab = ((ab)^{-1})^{-1} \in (H_1H_2)^{-1} \subseteq H_2^{-1}H_1^{-1} \subseteq H_2H_1,$$

因而 $H_1H_2 \subseteq H_2H_1$, 所以 $H_1H_2 = H_2H_1$. ■

6　子群的进一步思考

思考题 1.2.3　*若群 G 只有有限多个子群, 则 G 一定是有限群吗?*

是的, 既然群 G 只有有限多个子群, 因此 G 中所有元素的阶都是有限的, 否则, G 一定有无穷阶的元 a, 从而 G 有无穷多个子群, 矛盾.

任取 $a_1 \in G$, 则 $H_1 =< a_1 >$ 是 G 的一个有限子群. 取 $a_2 \in G \backslash < a_1 >$, 则 $H_2 =< a_2 >$ 是 G 的一个与 H_1 不同的有限子群. 再取 $a_3 \in G \backslash (< a_1 > \cup < a_2 >)$, 则 $H_3 =< a_3 >$ 是 G 的一个与 H_1 和 H_2 都不同的有限子群. 由于群 G 只有有限多个子群, 故上述过程只能做有限次, 因而一定存在某个正整数 n, 使得

$$G = H_1 \cup H_2 \cup \cdots \cup H_n.$$

因为每个 H_i 都是有限的, 所以 G 一定是有限群.

1902 年, Burnside[①]提出了著名的猜想: 如果群 G 是有限生成的, G 中的元素的阶都是有限的, 那么 G 是否一定是有限群?

Golod 在 1964 年给出了否定的答案[②].

思考题 1.2.4　*若群 G 的所有 (真) 子群都是交换群, 则 G 一定是交换群吗?*

不一定, 所有真子群都是交换群的非交换群称为内交换群, Miller 和 Moreno 在 1903 年就研究了内交换群[③].

1.3　置　换　群

解代数方程一直是数学研究的主要问题, 数学家们按次数从低到高地研究代数方程的可解性, 继而对方程的根的置换产生兴趣, 在几代数学家的努力下, 逐步深化了置换群的研究. 历史上最先被研究的群就是有限置换群, 它开始于 Lagrange 关于代数方程式求解的一般方法, 并随着伽罗瓦理论的需要而得到发展. Cauchy 的研究对于置换理论的发展和置换群的创立产生了重大影响, 从 1844 年到 1846 年共

① Burnside W. On an unsettled question in the theory of discontinuous groups. Quart. J. Pure Appl. Math., 1902, 33: 230–238.

② Golod E S. On nil-algebras and finitely approximable p-groups. Izv. Akad. Nauk SSSR Ser. Mat., 1964, 28: 273–276

③ Miller G A, Moreno H C. Non-abelian groups in which every subgroup is abelian. Trans. Amer. Math. Soc., 1903, 4: 398–404.

发表了二、三十篇论文, 在这些文章中他明确区分了排列和置换, 引进了置换的乘积和方幂的概念. 另外, 他还引进了单位置换和可逆置换.

容易知道, $\{2,1,4,5,3\}$ 这个排列可以看成集合 $\{1,2,3,4,5\}$ 到它自身的一个双射 σ, 它把 1 映成 2, 2 映成 1, 3 映成 4, 4 映成 5, 5 映成 3. 用列表的方法可以把这个映射表示成

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}.$$

1 置换群的定义

一般地, 有如下定义.

定义 1.3.1 *设 n 是一个自然数, 从集合 $\{1,2,3,\cdots,n\}$ 到它自身的一个双射称为 n 个文字的一个置换 (permutation), n 个文字的置换全体记为 S_n.*

从上面例子看出, 用列表法可把一个一般的置换 σ 表示为

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

这里的 $1,2,3,\cdots,n$ 并没有数量上的意义, 只是 n 个符号而已.

设 $\sigma,\tau \in S$, 规定 $\sigma\tau$ 为这两个映射的复合, 复合的次序是先 τ 后 σ, 即 $\sigma\tau$ 是这样的映射, 它把 i 映成 $\sigma[\tau(i)]$. 很明显, $\sigma\tau$ 仍然是 $\{1,2,3,\cdots,n\}$ 到其自身的一个双射. 所以这确实是个二元运算.

Ruffini 在 1799 年用归纳法证明了 S_n 中有 $n!$ 个置换.

命题 1.3.1 *S_n 在上面定义的二元运算下构成一个 $n!$ 阶的有限群.*

证明 根据复合映射的规则 $\sigma(\tau\pi) = (\sigma\tau)\pi$ 对任何 $\sigma,\tau,\pi \in S_n$ 成立, 故结合律成立.

记 e 或 (1) 为 $\{1,2,3,\cdots,n\}$ 到其自身的恒等映射, 即 $e(i) = i$ 对所有 $i = 1,2,3,\cdots,n$. 则 $e\sigma = \sigma e = \sigma$ 对任何 $\sigma \in S_n$ 成立, 因而 e 是 S_n 的单位元. 对任何 $\sigma \in S_n$, 由于它是一个双射, 它的逆映射存在, 它就是群论意义下 σ 的逆元, 所以 S_n 是一个群. ■

用列表法来作具体的群运算是很直接的. 如

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}^{-1}=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}.$$

n 次对称群是群概念的雏形, 是伽罗瓦在研究方程的根时首先提出的.

定义 1.3.2　S_n 称为 n 个文字的对称群 (symmetric group), S_n 的任何一个子群称为一个置换群 (permutation group).

例 1.3.1　对称群 S_3 的六个元素如下:

$$\sigma_0=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\quad \sigma_1=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\sigma_2=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\quad \sigma_3=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

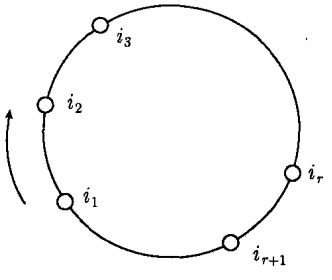
$$\sigma_4=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\quad \sigma_5=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

容易看出 $\sigma_1\sigma_2=\sigma_4$, 但 $\sigma_2\sigma_1=\sigma_3$, 故对称群 S_3 不是 Abel 群. 对称群 S_3 共有四个非平凡子群 $\{\sigma_0,\sigma_1\}$, $\{\sigma_0,\sigma_3\}$, $\{\sigma_0,\sigma_4\}$, $\{\sigma_0,\sigma_2,\sigma_5\}$.

实际上, 置换的列表表示法不简洁, 它的第一行显得有点多余. 如下面的置换

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}.$$

其实只不过把 1, 2 两个文字交换一下, 其他文字保持不动, 因此可以引进下面的概念.



定义 1.3.3　设 $i_1,i_2,\cdots,i_d$ 是 $\{1,2,3,\cdots,n\}$ 中的 d 个两两不同的文字, 若 $\sigma\in S_n$ 满足

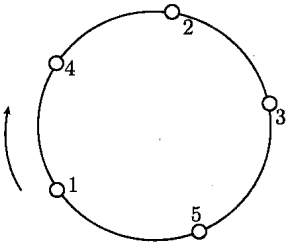
$$\sigma(i_1)=i_2,\sigma(i_2)=i_3,\cdots,\sigma(i_d)=i_1,$$

并且 $\sigma(i)=i$ 对 $\{1,2,3,\cdots,n\}$ 中的所有其他文字 i 成立, 则称 σ 为一个 d 轮换 (cycle), 记成 $(i_1i_2\cdots i_d)$. 特别地, 2 轮换 (i_1i_2) 称为对换 (transposition).

容易看出, 这样的记法不是唯一的, 如 $(i_1i_2\cdots i_d)$ 和 $(i_2i_3\cdots i_di_1)$ 表示相同的轮换.

每个循环的表达方法不唯一, 例如,

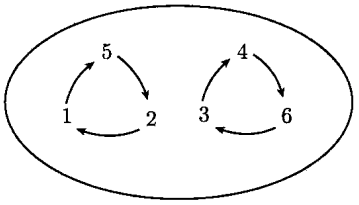
$$(14235)=(23514)=(51423).$$

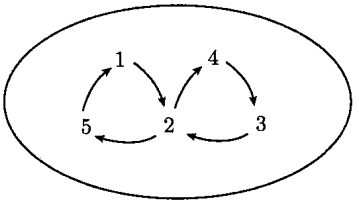


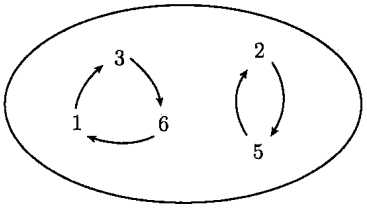
这是因为, 每个循环置换都可视为一个首尾相接的圆环, 因此循环中的每个文字都可以置于首位. 首位确定后, 整个循环置换的表达形式也就确定了. 不过习惯上, **总是将循环置换中出现的最小文字置在首位.**

定义 1.3.4 *若第一个轮换中的任何一个文字在第二个轮换中都不出现, 则称这两个轮换是不相交的.*

例 1.3.2 轮换 (152) 和 (346) 不相交, 但轮换 (512) 和 (243) 相交.







容易看出, 除恒等置换外, 任何一个轮换都可以写成若干个互不相交的轮换的乘积. 如

$$\begin{pmatrix}1&2&3&4&5&6\\3&5&6&4&2&1\end{pmatrix}=(136)(52).$$

两个置换相乘的运算不一定要通过列表法, 可以直接写出乘积的轮换表示式, 如 $\sigma=(152)(34)$, $\tau=(35)(41)$, 则

$$\sigma\tau=(152)(34)(35)(41).$$

2 置换的性质

命题 1.3.2 *任何一个置换可以表示成若干个对换的乘积.*

证明　明显地, 只需证明任意轮换可以表示成若干个对换的乘积. 实际上, 有

$$(i_1 i_2 \cdots i_d) = (i_1 i_2)(i_2 i_3) \cdots (i_{d-2} i_{d-1})(i_{d-1} i_d).$$ ■

例 1.3.3　$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 2 & 4 & 3 \end{pmatrix} = (25)(54)(36) = (23)(25)(54)(43)(36).$

Cauchy 在 1812 年就考虑了置换的符号差, 并在 1815 年的论文中区分了偶置换和奇置换.

定义 1.3.5　设 $\sigma \in S_n$, 令 $\operatorname{sgn}(\sigma) = (-1)^k$, 其中 k 是集合

$$\{(i,j) | 1 \leqslant i < j \leqslant n, \sigma(i) > \sigma(j)\}$$

中元素的个数. 把以上集合中的每个元素对 (i,j) 称为 σ 的逆序, 因此 k 就是 σ 的逆序数. 若 $\operatorname{sgn}(\sigma) = 1$, 则称 σ 为一个偶置换, 否则称为一个奇置换.

容易验证, 对于置换 σ:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix},$$

有

$$\operatorname{sgn}(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

由于

$$\begin{aligned} \operatorname{sgn}(\sigma\tau) &= \prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} \\ &= \prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \operatorname{sgn}\sigma \operatorname{sgn}\tau, \end{aligned}$$

故 $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \operatorname{sgn}\tau$, 对任意置换 σ 和 τ 都成立.

定义 1.3.6　S_n 所有偶置换构成 S_n 的子群, 称为 n 次交错群 (alternating group), 记作 A_n.

例 1.3.4　设

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}.$$

则 $(1,2)$, $(1,5)$, $(3,4)$, $(3,5)$, $(4,5)$ 是 σ 的全部逆序, 因此 $\operatorname{sgn}(\sigma)=-1$, 故 σ 是奇置换.

命题 1.3.3 *设 $\sigma\in S_n$, $\tau=(ij)$ 是一个对换, 其中 $i<j$. 若 σ 是偶置换, 则 $\sigma\tau$ 是奇置换; 若 σ 是奇置换, 则 $\sigma\tau$ 是偶置换.*

证明 先就 $j=i+1$ 的情形来证明. 将 $\sigma\tau$ 表示成

$$\begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(i) & \sigma(i+1) & \cdots & \sigma(n) \end{pmatrix}.$$

则

$$\sigma(i,i+1)=\begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(i+1) & \sigma(i) & \cdots & \sigma(n) \end{pmatrix}.$$

由此看出 $\sigma\tau$ 的逆序数比 σ 的逆序数多一或少一. 也就是说 $\sigma\tau$ 和 σ 的奇偶性相反.

对于一般情形 $1\leqslant i<j\leqslant n$, 根据等式

$$(ij)=(i,i+1)(i+1,i+2)\cdots(j-2,j-1)(j-1,j)\cdots(i+1,i+2)(i,i+1)$$

和已经证明的结果得知, $(ij)\sigma$ 和 σ 的奇偶性相反. ■

推论 1.3.1 *在对称群 $S_n(n>1)$ 中偶置换和奇置换各占一半.*

证明 设 A,B 分别是偶置换和奇置换所构成的集合, 因为 $\sigma\mapsto\sigma(12)$ 给出 A 到 B 的一个双射, 所以 A 和 B 所含元素个数相同. ■

推论 1.3.2 *一个置换是偶置换 (奇置换) 当且仅当它可表示成偶数 (奇数) 个对换的乘积.*

例 1.3.5 设

$$\sigma_1=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{pmatrix},\quad \sigma_2=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix},$$

$$\sigma_3=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 4 & 5 & 2 \end{pmatrix}.$$

(1) 求 σ_1^{-1}, σ_2^{-1}, σ_3^{-1};

(2) 求 $\sigma_2\sigma_1$ 和 $\sigma_3\sigma_2$;

(3) 试判断 σ_1, σ_2, σ_3 和 $\sigma_3\sigma_1$ 的奇偶性.

解　(1) $\sigma_1^{-1}=\begin{pmatrix}1&2&3&4&5&6\\2&6&3&5&4&1\end{pmatrix}$; $\sigma_2^{-1}=\begin{pmatrix}1&2&3&4&5&6\\3&1&2&6&5&4\end{pmatrix}$;

$\sigma_3^{-1}=\begin{pmatrix}1&2&3&4&5&6\\2&6&1&4&5&3\end{pmatrix}$.

$$(2)\ \sigma_2\sigma_1=\begin{pmatrix}1&2&3&4&5&6\\2&3&1&6&5&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\6&1&3&5&4&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6\\4&2&1&5&6&3\end{pmatrix};$$

$$\sigma_3\sigma_2=\begin{pmatrix}1&2&3&4&5&6\\3&1&6&4&5&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\2&3&1&6&5&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6\\1&6&3&2&5&4\end{pmatrix}.$$

(3) 由于 $\sigma_1=(12)(16)(45),\sigma_2=(13)(12)(46),\sigma_3=(12)(16)(13)$, 因而

$$\sigma_3\sigma_1=(1362)(162)(45)=(1236)(45)=(16)(13)(12)(45),$$

所以 σ_1, σ_2, σ_3 是奇置换, $\sigma_3\sigma_1$ 是偶置换. ■

1.4　陪　集

子群的陪集是伽罗瓦在 1830 年引入的.

1　陪集的定义

定义 1.4.1　*设 H 是 G 的一个子群, a 是 G 中的一个元素, 记 $aH=\{ah|h\in H\}$ 和 $Ha=\{ha|h\in H\}$, 则 aH 和 Ha 分别称为 H 在 G 中的左陪集* (left coset) *和右陪集* (right coset).

思考题 1.4.1　*设 H 是 G 的一个子群, 则 G 的左陪集 aH 和右陪集 Ha 是 G 的子群吗?*

例 1.4.1　设 $H=\{(1),(13)\}$, 则 H 为 S_3 的子群, 由于 $S_3=\{(1),(12),(13),(23),(123),(132)\}$, 故 $(12)H=\{(12),(132)\}$, 所以陪集 H 不是 S_3 的子群.

例 1.4.2　设 $G=GL_2(R)$, H 为所有的可逆二阶上三角矩阵所构成的子群,

$$g=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}.$$

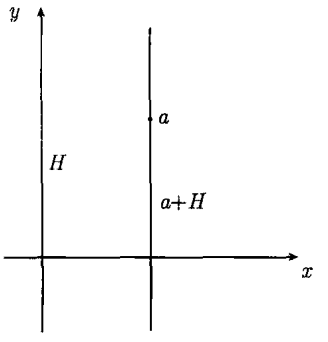
则

$$\begin{aligned}gH&=\left\{\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\begin{bmatrix}a & b\\ 0 & c\end{bmatrix}\Big|a\neq 0,c\neq 0\right\}\\&=\left\{\begin{bmatrix}a & b\\ a & b+c\end{bmatrix}\Big|a\neq 0,c\neq 0\right\}\\&=\left\{\begin{bmatrix}a & b\\ a & d\end{bmatrix}\Big|a\neq 0,d\neq b\right\},\end{aligned}$$

$$\begin{aligned}Hg&=\left\{\begin{bmatrix}a & b\\ 0 & c\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\Big|a\neq 0,c\neq 0\right\}\\&=\left\{\begin{bmatrix}a+b & b\\ c & c\end{bmatrix}\Big|a\neq 0,c\neq 0\right\}\\&=\left\{\begin{bmatrix}d & b\\ c & c\end{bmatrix}\Big|c\neq 0,d\neq b\right\}.\end{aligned}$$

例 1.4.3　$H=\{e,(123),(132)\}$ 是 S_3 的子群. 则 $(12)H=\{(12),(23),(13)\}$ 是 H 的一个左陪集 $H(12)=\{(12),(13),(23)\}$.

若将 $\mathbf{R}^2$ 看做是加法群 G, 取 OY 轴作为 $\mathbf{R}^2$ 的子群 H, 则对任意的 $a=(x_1,x_2)\in G$, 陪集 $a+H$ 就是过点 (x_1,x_2), 并且平行 OY 轴的直线. 由于 G 的子群一定经过原点, 故容易看出陪集 $a+H$ 不一定是 G 的子群.



非齐次线性常微分方程的解还可以看做对应的齐次线性常微分方程的解的陪集.

例 1.4.4　设 $C^1(-\infty,+\infty)$ 为所有可微函数全体, 则它在函数加法下是一个群, 考虑常微分方程 $\dfrac{\mathrm{d}y}{\mathrm{d}x}+xy=x^3$ 的解时, 容易知道方程 $\dfrac{\mathrm{d}y}{\mathrm{d}x}+xy=0$ 的解 $H=\{c\mathrm{e}^{-\frac{x^2}{2}}|c\in\mathrm{R}\}$ 为 $C^1(-\infty,+\infty)$ 的子群. 不难验证 x^2-2 是 $\dfrac{\mathrm{d}y}{\mathrm{d}x}+xy=x^3$ 的一个特解, 因此子群 H 关于 x^2-2 的陪集 $(x^2-2)+H$ 就是微分方程 $\dfrac{\mathrm{d}y}{\mathrm{d}x}+xy=x^3$ 的全部解.

2　陪集的性质

陪集具有如下基本性质.

性质 1.4.1　*设 $a,b\in G$, H 是 G 的子群, 则映射 $f:aH\to bH, g\mapsto ba^{-1}g$ 是双射.*

证明　容易看出映射 f 是有意义的. 定义映射 $\varphi:bH\to aH, g\mapsto ab^{-1}g$, 则 $\varphi\circ f$ 和 $f\circ\varphi$ 都是恒等映射, 所以 f 是双射. ■

推论 1.4.1　*设 $a,b\in G$, H 是 G 的子群, 则 H, aH 和 bH 有相同的元素个数.*

思考题 1.4.2　*设 H 是 G 的一个子群, $a\notin H$, 则 G 的左陪集 aH 和 H 有公共的元素吗?*

没有. 假如 $h\in H\cap aH$, 则存在 $h_1\in aH$, 使得 $h=ah_1$, 故 $a=hh_1^{-1}\in H$, 但这与 $a\notin H$ 矛盾, 所以 $H\cap aH$ 是空集.

思考题 1.4.3　*设 H 是 G 的一个子群, $a,b\in G$, 若 b 不是 aH 中的元素, 则 G 的左陪集 aH 和 bH 有公共的元素吗?*

没有. 从下面命题的证明容易看出.

命题 1.4.1　*$aH=bH$ 当且仅当 $a^{-1}b\in H$.*

证明　设 $aH=bH, b\in aH$, 因此存在 $h\in H$, 使得 $b=ah$, 所以 $a^{-1}b=h\in H$.

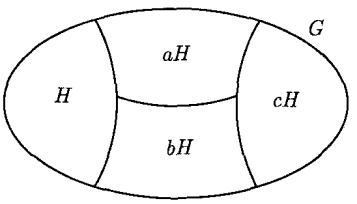
反过来, 设 $a^{-1}b\in H$, 令 $h=a^{-1}b$, 则 $h\in H$, 故 $b=ah\in aH$. 从而 $bH\subseteq aH$. 另外, $b^{-1}a=(a^{-1}b)^{-1}\in H$, 因此, $aH\subseteq bH$, 所以 $aH=bH$. ■

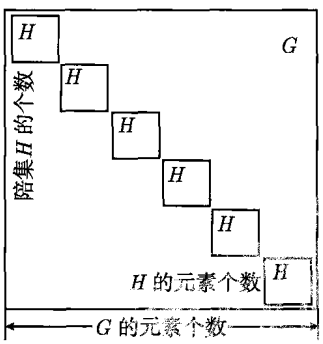
推论 1.4.2　*若 $aH\cap bH\neq\varnothing$, 则 $aH=bH$.*

证明　设 $g \in aH \cap bH$. 则 $g = ah = bh'$, 其中 $h, h' \in H$. 因此 $a^{-1}b = hh'^{-1} \in H$, 所以 $aH = bH$. ■

3 Lagrange 定理

由于 $a \in aH$ 对任何 $a \in G$ 成立, 故 G 中每个元素都属于 H 的一个左陪集, 所以 G 可以表示成一些互不相交的左陪集的并, 也就是说 H 的左陪集给出了 G 的一种**划分**(partition).





定义 1.4.2　*群 G 的子群 H 的陪集个数称为 H 在 G 中的指数* (index), *记作* $[G : H]$, *这里的* $[G : H]$ *可以是某个自然数或* ∞.

Lagrange 证明了置换群的任一元的阶是该群的阶的因子, Jordan 利用把一个群分解成其子群的陪集的方法证明有限群的任一子群的阶是该群的阶的因子.

定理 1.4.1(Lagrange)　*设 H 是有限群 G 的一个子群, 则* $|G| = |H|[G : H]$.

证明　这是因为每个陪集都含 $|H|$ 个元素. ■

推论 1.4.3　*设 G 是一个 n 阶有限群, $a \in G$, 则 a 的阶整除 $|G|$.*

证明　由于子群 $< a >$ 的元素个数就是 a 的阶, 故 a 的阶整除 $|G|$. ■

Joseph-Louis Lagrange(1736—1813)

思考题 1.4.4　Lagrange 定理的逆命题成立吗?

给定一个有限群 G 和一个整除 G 的阶的整数 m, G 并不一定有阶数为 m 的子群. 最简单的例子是 4 次对称群 S_4 中所有偶置换所构成的群 A_4, 它的阶是 12, 但对于 12 的因数 6, A_4 没有 6 阶的子群.

定义 1.4.3　*设 G 为有限群, 若每个整除 G 的阶的整数 m, G 一定有阶数为 m 的子群, 则称群 G 是* Lagrange *的.*

这类群的研究可见 McLain D H[①]和 Humphreys J F[②].

4 Lagrange 定理的应用

下面来看看 Lagrange 定理的应用.

例 1.4.5　试证明素数阶的有限群是循环群.

证明　设 $p=|G|$. 任取 $a\in G$, $a\neq e$. 则 $o(a)>1$ 且 $o(a)|p$, 由于 p 是素数, 因此 $o(a)=p$, 所以 $G=<a>$. ■

例 1.4.6　设 G 是有限群, $a\in G$, 试证明 $a^{|G|}=e$.

证明　由 Lagrange 定理可知 a 的阶 $o(a)$ 整除 G 的阶 $|G|$, 因为 $a^{o(a)}=e$, 所以 $a^{|G|}=e$. ■

当 a,b 是整数时, 若 m 整除 $a-b$, 则称 a 和 b 是同余的, 记为 $a\equiv b(\mathrm{mod}\, m)$. Fermat 1636 年在研究完全数时发现 2^p-2 能被素数 p 整除. 之后不久, 即 1640 年 10 月 18 日, 致信 Bernard Frenicle de Bessy, Fermat 说他能证明更一般的情况: 如果 p 是一个素数, a 是和 p 互素的任意整数, 那么 $a^{p-1}-1$ 能被 p 整除, 即 $a^{p-1}\equiv 1(\mathrm{mod}\, p)$. 这就是现在所说的 Fermat 小定理. 1736 年, Eider 证明了 Fermat 小定理, 随后 1750 年和 1761 年又分别给出了两个证明, 其中前两个证明利用了归纳法和二项式公式. 有趣的是利用上面的结论, 还可以给出数论中的 Fermat 小定理 (Fermat's little theorem) 一个简短的证明.

定理 1.4.2(Fermat 小定理)　*若 p 是素数, 并且 a 不是 p 的倍数, 则*

$$a^{p-1}\equiv 1(\mathrm{mod}\, p).$$

证明　由于 p 是素数, 故 $\mathbf{Z}_p^*=\{\overline{1},\overline{2},\cdots,\overline{p-1}\}$ 在乘法下是一个乘法群. 由 a 不是 p 的倍数可知 $\overline{a}\in\mathbf{Z}_p^*$, 从而 $\overline{a}$ 的 $|\mathbf{Z}_p^*|$ 次方等于 $\overline{1}$, 故 $\overline{a^{p-1}}=(\overline{a})^{p-1}=\overline{1}$, 所以 $(\overline{a})^{p-1}\equiv 1(\mathrm{mod}p)$. ■

思考题 1.4.5　*设 H,K 是群 G 的两个有限子群, HK 一定是 G 的子群吗?*

在 H,K 是群 G 的两个有限子群时, 无论 HK 是不是 G 的子群, 一样可以用群的阶的记法, 用 $|HK|$ 来记 HK 中元素的个数.

① McLain D H. The existence of subgroups of given order in finite groups. Proc. Cambridge Philos. Soc., 1957, 53: 278–285.

② Humphreys J F. On groups satisfying the converse of Lagrange's theorem. Proc. Cambridge Philos. Soc., 1974, 75: 25–32.

定理 1.4.3　*设 H, K 是群 G 的两个有限子群, 则*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

证明　明显地, HK 的元素个数最多不会超过 $|H||K|$. 由于 HK 中的元素都具有形式 $hk(h \in H, k \in K)$, 故只需考虑对于 $h \in H, k \in K$, 与 hk 相等的元素有多少, 如果 $h, h' \in H, k, k' \in K$, $hk = h'k'$, 那么 $h'^{-1}h = k'k^{-1}$, 因此记 $c = h'^{-1}h = k'k^{-1}$ 时, 有 $c \in H \cap K$, 并且 $h = h'c, k = c^{-1}k'$.

反过来, 对任意的 $c \in H \cap K$, 对于 $h \in H, k \in K$, 有 $h' = hc^{-1} \in H, k' = ck \in K$, 使得 $hk = h'k'$. 另外, 容易知道, 当 $c_1, c_2 \in H \cap K$, $c_1 \neq c_2$ 时, 有

$$h'_1 = hc_1^{-1} \neq h'_2 = hc_2^{-1}, k'_1 = c_1k \neq k'_1 = c_2k.$$

对任意选定的 $h \in H, k \in K$, 有且仅有 $|H \cap K|$ 个 H 和 K 中的元素, 它们的乘积与 hk 相等, 因此 $|HK|$ 与 $|H \cap K|$ 的乘积就等于 $|H||K|$, 所以定理成立. ■

利用上面的定理, 还可以给思考题 1.4.5 一个解答.

例 1.4.7　在 $S_3 = \{(1), (12), (13), (23), (123), (132)$ 中, $H = \{(1), (12)\}$, $K = \{(1), (13)\}$ 是 S_3 的子群, 试证明 HK 不是 S_3 的子群.

证明　由于 $H \cap K = \{(1)\}, |H| = 2, |K| = 2$, 故

$$|HK| = \frac{|H||K|}{|H \cap K|} = 4,$$

从而 $HK = \{(1), (13), (12), (132)\}$. 由 4 不能整除 6 和 Lagrange 定理可知, HK 不是 S_3 的子群. ■

5　双陪集的定义

双陪集的特殊例子很早就出现 Cauchy 的工作中, 但在群论中系统的考虑归于 Frobenius.

定义 1.4.4　*设 H, K 是有限群 G 的两个子群, 称形如 HaK 的子集为 G 的双陪集* (double coset).

设 H, K 是有限群 G 的两个子群, 不难证明双陪集 HaK 与 HbK 要么相等, 要么不相交.

思考题 1.4.6　双陪集有跟陪集类似的性质吗?

例 1.4.8　在对称群 S_3, 取子群 $H=\{(1),(12)\}$ 和 $K=\{(1),(13)\}$, 则

(1) 的双陪集为 $H(1)K=\{(1),(12),(13),(132)\}$, (23) 的双陪集 $H(23)K=\{(1)(23)(1),(1)(23)(13),(12)(23)(1),(12)(23)(13))\}=\{(23),(123)\}$.

因此, 关于同样两个子群的不同元素的双陪集的阶可以不一样, 并且双陪集的阶也不一定整除群的阶.

1.5　正规子群

1830 年伽罗瓦在研究代数方程的根的性质的过程中, 发现了一类很重要的子群, 这就是正规子群. 他证明了对于每个代数方程都对应一个有限群, 方程的根的性质依赖于方程的群的正规子群的特征, 从而正规子群提供了它对应的代数方程的解的性质的基础.

先来看看需要引入正规子群这个概念的原因, 设 H 是群 G 的一个子群, 令 Ω 为 H 在 G 中的左陪集全体所构成的集合. 设 $aH\in\Omega$, 则 a 称为陪集 aH 的一个**代表元**(representative).

设 $aH,bH\in\Omega$, 能不能将 aH 和 bH 的乘积定义为 $(ab)H$? 由于代表元是不唯一的, 故这个定义左陪集 $(ab)H$ 必须与代表元 a 和 b 的选取无关.

设 a' 和 b' 分别为 aH 和 bH 的其他代表元, 即 $a'=ah,b'=bk$, 其中 $h,k\in H$. 为使 $(ab)H=(a'b')H$, 必须 $(ab)^{-1}(a'b')\in H$, 即 $b^{-1}a^{-1}ahbk=b^{-1}hbk\in H$. 也就是说 $b^{-1}hb\in H$ 必须对所有 $b\in G$ 和所有 $h\in H$ 成立. 具有这种性质的子群是伽罗瓦发现的, 称之为正规子群.

1　正规子群的定义

定义 1.5.1　*群 H 为 G 的子群, 若对任意的 $a\in G$, 都有 $aH=Ha$, 则称 H 为 G 的一个正规子群* (normal subgroup), *记作 $H\triangleleft G$.*

命题 1.5.1　*设 H 是群 G 的子群, 则 H 是群 G 的正规子群当且仅当 $aHa^{-1}=H$ 对任意 $a\in G$ 成立.*

证明　若 $aHa^{-1}=H$ 对任意 $a\in G$ 成立, 则对任意 $h\in H$, 都有

$$ah = (aha^{-1})a \in Ha.$$

故 $aH \subseteq Ha$, 同理 $Ha \subseteq aH$, 所以 H 是群 G 的正规子群.

若 $aH = Ha$ 对任意 $a \in G$ 成立, 则对任意 $a \in G, h \in H$, ha 属于 aH, 即 $ha = ah'$ 对某个 $h' \in H$ 成立, 故 $a^{-1}ha = h' \in H$, 因此 $aHa^{-1} \subseteq H$. 对任意 $h \in H$, 由 $aH = Ha$ 可知 $a^{-1}H = Ha^{-1}$, 因此存在 $h' \in H$ 使得 $a^{-1}h = h'a^{-1}$ 成立, 故

$$h = (aa^{-1})h = a(a^{-1}h) = ah'a^{-1} \in aHa^{-1}.$$

因而 $H \subseteq aHa^{-1}$, 所以 $aHa^{-1} = H$ 对任意 $a \in G$ 成立. ■

当 $H \triangleleft G$ 时, 左陪集和右陪集这两个概念等价, 因此可以把它们简称为**陪集**.

伽罗瓦首次证明群 G 关于正规子群 H 的陪集构成一个群, 这个群称为商群 G/H. 商群记号 G/H 是 Jordan 在 1873 年引进的.

2 商群的定义

定义 1.5.2 *设 H 是群 G 的正规子群, H 的所有陪集在运算 $(aH)(bH) = (ab)H$ 下是一个群, 称为 G 关于 H 的商群* (quotient group), *记作 G/H.*

容易知道, 当 G 是有限群时, 有

$$|G/H| = [G : H] = \frac{|G|}{|H|}.$$

商群 G/H 中的元素是陪集 aH, 通常可以记作 $\overline{a}$ 或 $[a]$, 称为由元素 a 所代表的陪集.

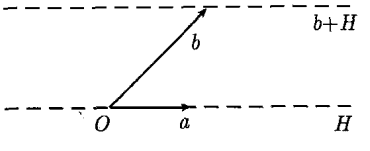
在很多 Abel 群中, 群运算用加号 $+$ 表示, 这时陪集应写成 $a + H$.

商群 G/H 的全体元素可以写为

$$a_1H, a_2H, \cdots,$$

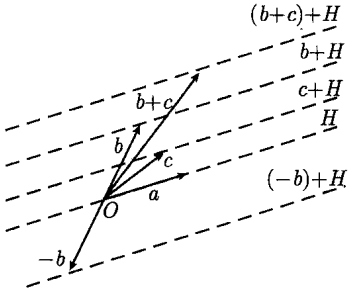
其中 $a_i^{-1}a_j \notin H$ 对任何 $i \neq j$ 成立, 并且对任意 $a \in G$, 存在 i 使 $a^{-1}a_i \in H$.

商群 G/H 是什么呢? 先来看看下面这个比较直观的例子.



设 G 表示平面上从点 O 出发的所有向量, 则在向量的加法下 G 构成加法群. 容易知道, 对于取定的向量 a, 端点在延长线上的所有向量就构成 G 包含 a 的子群 H.

任取 $b \notin H$, 则向量 b 所在的陪集 $b+H$ 就是过 b 的端点并且与直线 a 平行的所有向量.



由于 G 是交换群, 故 H 是 G 的正规子群, 商群 G/H 由一切平行于 a 的直线组成.

两条平行线 $b+H$ 和 $c+H$ 的和为过向量 $b+c$ 的端点平行于 a 的直线 $(b+c)+H$, 商群 G/H 的零元就是 a 所在的直线 H, $b+H$ 的逆元就是 $(-b)+H$, 它与 $b+H$ 关于直线 a 对称.

例 1.5.1　K 上的行列式等于 1 的 n 阶方阵群 $SL_n(K)$ 是 n 阶可逆矩阵群 $GL_n(K)$ 的正规子群. 但 n 阶上三角矩阵全体所构成的子群不是 n 阶可逆矩阵群 $GL_n(K)$ 的正规子群.

例 1.5.2　$H=\{cI_n | c \in K, c \neq 0\}$ 是 n 阶可逆矩阵群 $GL_n(K)$ 的正规子群, 商群 $GL_n(K)/H$ 通常记作 $PGL_n(K)$, 称为**射影一般线性群**(projective general linear group).

例 1.5.3　令 $H=\{e,(123),(132)\} \subset S_3$, 则 H 是 S_3 的正规子群, 商群 S_3/H 含两个元素 H 和 $(12)H$, 第一个元素是单位元.

例 1.5.4　设 n 是大于 1 的自然数, 令 nZ 为被 n 整除的整数全体所构成的集合, 则 Z/nZ 是一个 n 阶循环群, 其元素可列举如下

$$\overline{0},\overline{1},\overline{2},\cdots,\overline{n-1},$$

其中 $\overline{1}$ 可选作这个循环群的生成元.

下面的问题是很有意思的.

思考题 1.5.1　*如果群 G 中每个元的阶都是有限的, 那么群 G 的阶一定是有限的吗?*

不一定. 利用商群, 可以容易地构造出下面的例子.

例 1.5.5　记 $\mathbf{Q}$ 是全体有理数在加法下构成 Abel 群, 商群 $\mathbf{Q}/\mathbf{Z}$ 是无限群, 但是每个元素的阶是有限的. 实际上, 对任意有理数 $a \in \mathbf{Q}/\mathbf{Z}$, 存在整数 m 和 n, 使得 $a=\dfrac{n}{m}+\mathbf{Z}$, 从而 $ma=n+\mathbf{Z}=0+\mathbf{Z}$, 因此 a 的阶是有限的. 但明显地, 群 $\mathbf{Q}/\mathbf{Z}$

是无限群.

思考题 1.5.2 设 H 不是 G 的正规子群, 二元运算 $(aH)(bH)=(ab)H$ 有意义吗?

例 1.5.6 $K=\{e,(12)\}$ 是 S_3 的一个二阶子群, 它的左陪集为

$$K=eK,$$

$$(13)K=\{(13),(123)\},$$

$$(23)K=\{(23),(132)\}.$$

把 $(13)K$ 中每个元素和 $(23)K$ 中每个元素分别相乘, 得

$$(132),(23),(12),e,$$

它们不构成陪集. 这个例子表明对于非正规子群陪集的集合不能定义合理的乘法.

容易知道, 平凡子群总是正规子群. 若群 G 是交换群, 则它的任意子群都一定是正规子群. 反过来呢?

思考题 1.5.3 若群 G 的任意子群都一定是正规子群, 群 G 一定是交换群吗?

不一定. 有的非交换群的子群都是正规子群, 这种群称为**Hamilton 群**①. 在复数域上取 4 个 2 阶矩阵:

$$I=\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad A=\begin{bmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{bmatrix},\quad B=\begin{bmatrix}0&1\\-1&0\end{bmatrix},\quad C=\begin{bmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{bmatrix}$$

在矩阵的乘法下生成一个 8 元群

$$G=\{\pm I,\pm A,\pm B,\pm C\},$$

则 G 只有一个 2 元子群和三个 4 元子群, 即

$$\{I,-I\},\{A,-I,-A,I\},$$

$$\{B,-I,-B,I\},\{C,-I,-C,I\}.$$

不难验证这4个子群都是G的正规子群, 但G不是交换群, 这是最小的 Hamilton 群.

① Cappitt D. Generalized Dedekind groups. J. Algebra, 1971, 17: 310–316.

3　正规子群的性质

性质 1.5.1　设 H 是 G 的正规子群, K 是 G 的包含 H 的子群, 则 H 是 K 的正规子群.

定义 1.5.3　设 G 是一个群, $g \in G$, 形如 $a^{-1}ga$(这里 $a \in G$) 的元素称为 g 的共轭元. 若 H 是 G 的一个子群, 则 $a^{-1}Ha$ 为 G 的子群, 称为 H 的一个共轭子群 (conjugate subgroup).

性质 1.5.2　H 是群 G 的正规子群当且仅当 H 的所有共轭子群等于 H.

例 1.5.7　设 H 是群 G 的子群, 满足 $[G:H]=2$, 试证明 H 是群 G 的正规子群.

证明　当 $a \in H$ 时, 明显地有 $aH = Ha$. 若 $a \notin H$, 则 aH 是 H 的一个不同于 H 的左陪集. 由于 $[G:H]=2$, H 在 G 中只有两个左陪集, 故 $aH = G\backslash H$. 同理 $Ha = G\backslash H$, 所以 $aH = Ha$, 因此 H 是群 G 的正规子群. ■

明显地, 任何一个群 G 的中心 $C(G)$ 总是 G 的正规子群, 正规子群具有下面一些性质.

性质 1.5.3　设 H 和 K 为群 G 的子群, 则

(1) 若 H 和 K 都是群 G 的正规子群, 则 H 与 K 的乘积 HK 也是群 G 的正规子群.

(2) 若 H 和 K 都是群 G 的正规子群, 则 H 与 K 的交也是群 G 的正规子群.

(3) 若 H 和 K 都是群 G 的正规子群, 并且 H 与 K 的交为 $\{e\}$, 则 $hk = kh$ 对任意的 $h \in H$ 和任意的 $k \in K$ 成立.

例 1.5.8　设 S 是 G 的一个子集, 若 $a^{-1}sa \in S$ 对任意 $a \in G, s \in S$ 成立, 试证明由 S 生成的子群是 G 的正规子群.

证明　设 b 是 S 生成的子群 $< S >$ 中任意一个元素, 则

$$b = s_1^{k_1} \cdots s_n^{k_n} \in S,$$

这里 $s_i \in S, k_j$ 为整数. 不妨设 $k_1 > 0$, $k_2 < 0$, $k_n > 0$, 则

$$\begin{aligned} a^{-1}ba =& (a^{-1}s_1a)(a^{-1}s_1a)\cdots(a^{-1}s_1a)(a^{-1}s_2a)^{-1}(a^{-1}s_2a)^{-1}\cdots \\ & (a^{-1}s_2a)^{-1}\cdots(a^{-1}s_na) \end{aligned}$$

(上式中 $a^{-1}s_1a$ 有 k_1 个, $a^{-1}s_2a$ 有 $|k_2|$ 个, $\cdots$, $a^{-1}s_na$ 有 k_n 个). 由于右边的每一项都属于 $< S >$, 从而 $a^{-1}ba \in < S >$, 所以由 S 生成的子群是 G 的正规子群. ■

4 换位子群

Dedekind 在 1897 年研究群论时引进了换位子群这个概念, 并证明换位子群一定是正规的.

定义 1.5.4 *群 G 中可以写成 $a^{-1}b^{-1}ab$ 形式的元素称为换位子, 所有 G 的有限个换位子的乘积构成 G 的正规子群, 称为 G 的换位子群* (commutataor subgroub) *或导群* (derived group), *记为 $[G,G]$ 或 G'.*

例 1.5.9 不难验证对称群 S_3 的换位子群为 $[S_3,S_3]=A_3$.

性质 1.5.4 (1) *若 H 是群 G 的子群, 则 $H' \subseteq G'$;*

(2) *若 H 是群 G 的正规子群, 则 $(G/H)' = G'H/H$.*

证明 (1) 由定义容易知道 $H' \subseteq G'$ 成立.

(2) $(G/H)'$ 是所有形如 $a^{-1}Hb^{-1}HaHbH = a^{-1}b^{-1}abH$ 的元的有限乘积, 由于 $a^{-1}b^{-1}ab \in G'$, 故 $a^{-1}b^{-1}abH \in G'H/H$, 从而 $(G/H)' \subseteq G'H/H$.

反过来, 对任意 $cH \in G'H/H$, 有 $c \in G'$, 故 $c = \prod\limits_{i=1}^{n} a_i^{-1}b_i^{-1}a_ib_i, a_i, b_i \in G$, 因此

$$cH = \left(\prod_{i=1}^{n} a_i^{-1}b_i^{-1}a_ib_i\right)H = \prod_{i=1}^{n}(a_i^{-1}Hb_i^{-1}Ha_iHb_iH) \in (G/H)',$$

从而 $G'H/H \subseteq (G/H)'$. 综合上述, 有 $(G/H)' = G'H/H$. ■

利用群 G 的换位子群 $[G,G]$ 或 G', 还可以将一般群 G 进行 "交换" 化, 其实不难验证 G/G' 就是交换群.

实际上, 对任意的 $a, b \in G$, 有 $\overline{a}\overline{b} = aG'bG' = abG' = G'ab = G'ab(a^{-1}b^{-1}ba) = G'(aba^{-1}b^{-1})ba$, 由 G' 是群 G 的换位子群可知, $aba^{-1}b^{-1} \in G'$, 从而

$$G'(aba^{-1}b^{-1})ba = G'ba = G'bG'a = \overline{b}\overline{a}.$$

所以 G/G' 就是交换群.

另外, 如果 H 是 G 的正规子群, G/H 是交换群, 那么对任意的 $a, b \in G$, 有

$$Haba^{-1}b^{-1} = HaHbHa^{-1}Hb^{-1}.$$

由于 G/H 是交换群, 故

$$HaHbHa^{-1}Hb^{-1} = HaHa^{-1}HbHb^{-1} = H(aa^{-1})H(bb^{-1}) = H.$$

因此由 $Haba^{-1}b^{-1} = H$ 可得, $aba^{-1}b^{-1} \in H$, 因而 H 一定包含 G 的换位子群 G', 所以换位子群 G' 是使得 G 关于它的正规子群的商群成为交换群的最小正规子群.

思考题 1.5.4　*设 H 是群 G 的子群, 若 H 的换位子群与 G 的换位子群一样, 则是否一定有 $H = G$?*

不一定, 其实不难看出, 当 G 是交换群时, 对于 G 的任意真子群 H, 都有 $H' = G' = \{e\}$.

定义 1.5.5　*设 H 是群 G 的子群, 称 $N_G(H) = \{a \in G | a^{-1}Ha = H\}$ 为 H 在 G 中的正规化子群* (normalizer).

例 1.5.10　设 H 是 G 的一个子群, 试证明正规化子群 $N_G(H)$ 是 G 的子群, 并且 H 是正规化子群 $N_G(H)$ 的正规子群.

证明　先证 $N_G(H)$ 是 G 的子群.

设 $a \in N_G(H)$, 则 $a^{-1}Ha = H$, 故 $aHa^{-1} = H$, 从而 $a^{-1} \in N_G(H)$. 因此正规化子群 $N_G(H)$ 对求逆封闭.

设 $a, b \in N_G(H)$. 则 $(ab)^{-1}H(ab) = b^{-1}(a^{-1}Ha)b = b^{-1}Hb = H$. 故 $ab \in N_G(H)$, 即 $N_G(H)$ 对乘法封闭, 因此正规化子群是 G 的子群.

根据正规化子群 $N_G(H)$ 的定义 $N_G(H) = \{a \in G | a^{-1}Ha = H\}$, 容易知道 H 是正规化子群 $N_G(H)$ 的正规子群. ■

思考题 1.5.5　*若 H_1 是 H_2 的正规子群, H_2 是 G 的正规子群, 则 H_1 是否一定是 G 的正规子群呢?*

不一定, 容易验证, $H_1 = \{e, (12)(34)\}$ 是 $H_2 = \{e, (12)(34), (13)(24), (14)(23)\}$ 的正规子群, H_2 是对称群 S_4 的正规子群, 但 H_1 不是对称群 S_4 的正规子群.

5　正规子群的推广

由于正规子群在有限群的研究中有着非常重要的作用, 故很多数学家引入了与正规性质密切相关但性质弱一些的概念. Ore 在 1939 年定义了**拟正规子群**(quasi-

normal subgroup), 设 H 是 G 的子群, 若对 G 的任意子群 K, 都有 $HK = KH$, 则称 H 为 G 的拟正规子群①. Kegel 在 1962 年引入了比拟正规子群更弱的正规性, 设 H 是 G 的子群, 若 H 与 G 的所有 Sylow 子群 K 都可交换, 即有 $HK = KH$, 则称 H 为 G 的 s-**拟正规子群**②.

如果群 G 有一个循环的正规子群 H, 使得 G/H 也是循环群, 则称 G 为**亚循环群**(metacyclic group). 若有限群 G 的每个 Sylow 子群都是循环群, 则 G 一定是亚循环群. 亚循环群的性质已经得到了较深入的讨论③.

1.6 交 错 群

交错群 A_n 是对称群 S_n 中所有偶置换所构成的群, 交错群 A_n 是 $\frac{n!}{2}$ 阶群, 它具有下面的一些性质.

1 交错群的性质

定理 1.6.1 *当 $n > 1$ 时, 交错群 A_n 是对称群 S_n 的正规子群.*

证明 (1) 先证 A_n 是 S_n 的子群. 设 $\sigma, \tau \in A_n$, 则 σ, τ 可以表示成 $2l$ 和 $2m$ 个对换的乘积, 故 $\sigma\tau$ 可表示成 $2(l+m)$ 个对换的乘积, 因而 $\sigma\tau \in A_n$. 类似可证 A_n 对求逆也封闭, 所以 A_n 是对称群 S_n 的子群.

(2) 下面证明 A_n 是对称群 S_n 的正规子群. 由于 $\sigma \mapsto (12)\sigma$ 给出 A_n 到奇置换集合的一个双射, 而每一个置换不是偶置换就是奇置换, 故 $S_n = A_n \cup (12)A_n$, 因此 $(S_n : A_n) = 2$. 所以, A_n 是对称群 S_n 的正规子群. ■

2 单群的定义和例子

伽罗瓦将没有非平凡正规子群的群称为单群, 他还提出了一个猜想: 阶是合成数的最小单群是 60 阶的群.

定义 1.6.1 *一个不包含非平凡正规子群的群称为单群* (simple group).

---

① Ore O. Contributions to the theory of groups. Duck Math. J., 1939, 5: 431–460.

② Kegal O H. Sylow grouppen and subnormalteiler endlicher grouppen. Math. Z., 1962, 78: 202–221.

③ Shmel'kin A L. Metacyclic group // Hazewinkel, Michiel, Encyclopaedia of Mathematics. Springer, 2001.

推论 1.6.1　当 $n>2$ 时, 对称群 S_n 不是单群.

对于 A_5, 不难验证, 下面引理成立.

引理 1.6.1　交错群 A_5 中所有的 3-循环置换共轭.

引理 1.6.2　交错群 A_5 的每个元素或是 3-循环置换或是一些 3-循环置换的乘积.

定理 1.6.2　交错群 A_5 是单群.

证明　设 H 是交错群 A_5 的正规子群, 且 $H\neq\{(1)\}$. 若 H 含有 3-循环置换, 由 H 是 A_5 的正规子群可知, H 含有它所有的共轭. 根据上面引理, H 含有每个 3-循环置换. 因此要证明 $H=A_5$, 只需证明 H 含有 3-循环置换.

由于 $H\neq\{(1)\}$, 故它含有某个 $\sigma\neq(1)$. 不妨假设 H 含有

$$\sigma=(123),\ \sigma=(12)(34)\ 或\ \sigma=(12345).$$

情形一. 若 σ 是 3-循环置换, 则 H 含有 3-循环置换.

情形二. 若 $\sigma=(12)(34)\in H$, 令 $\beta=(345)$, $\tau=\beta\alpha\beta^{-1}$, 则 $\tau=(12)(45)\in H$, 因而 $\sigma\tau=(345)\in H$, 故 $\sigma\tau$ 是 3-循环置换, 因此 H 含有 3-循环置换.

情形三. 若 $\sigma=(12345)\in H$, 令 $\tau=(123)$, $\tau=\beta\alpha\beta^{-1}$, 则

$$\tau=(23145)\in H.$$

因而 $\tau\sigma^{-1}=(23145)(54321)=(124)\in H$, 故 $\tau\sigma^{-1}$ 是 3-循环置换, 因此 H 含有 3-循环置换.

至此已经证明, 在所有的情形中, H 均含有 3-循环置换, 故 $H=A_5$. 因此, 交错群 A_5 的正规子群只有 $\{(1)\}$ 和 A_5 本身, 所以交错群 A_5 是单群. ■

类似地, 对于交错群 A_n, 有如下结论成立.

引理 1.6.3　当 $n>2$ 时, 对称群 S_n 可由所有的对换生成, 即

$$S_n=<(12),(13),\cdots,(1n)>.$$

交错群 A_n 可由所有的 3 轮换生成, 即 $A_n=<(123),(124),\cdots,(12n)>$.

利用上面引理, 可以证明如下定理.

定理 1.6.3 当 $n \geqslant 5$ 时, 交错群 A_n 是单群.

Feit 和 Thompson 在 1963 年证明了著名的 Burnside 猜想: 非交换的单群的元素个数一定是偶数①.

1.7 群的同态

群的同态和它的核的明确研究是 Gapelli 在 1878 年开始的.

1 群同态的基本概念

定义 1.7.1 设 G_1, G_2 为两个群, 映射 $f: G_1 \to G_2$, 若 $f(ab) = f(a)f(b)$ 对任意 $a, b \in G_1$ 成立, 则称 f 为同态 (homomorphism).

定义 1.7.2 设 G_1, G_2 为两个群, 分别以 e_1 和 e_2 为单位元, f 为 G_1 到 G_2 的同态, 记 $\mathrm{Ker}(f) = \{a \in G_1 | f(a) = e_2\}$, 称为 f 的核 (kernel). f 是单射当且仅当 $\mathrm{Ker}(f) = \{e_1\}$, 这时称 f 为一个单同态 (monomorphism).

记 $\mathrm{Im}(f) = \{f(a) | a \in G_1\}$, 这是 G_2 的一个子群, 称为 f 的像 (image). f 是满射当且仅当 $\mathrm{Im}(f) = G_2$, 这时 f 称为一个满同态 (epimorphism).

2 群同态的性质

容易证明, 若 f 为 G_1 到 G_2 的同态, 则 f 的核是 G_1 的一个正规子群.

性质 1.7.1 设 G_1, G_2 为两个群, 分别以 e_1 和 e_2 为单位元, $f: G_1 \to G_2$ 是一个群同态, 则

(1) f 将 G_1 的单位元映为 G_2 的单位元;

(2) f 将 $a \in G_1$ 的逆元映为 G_2 中 $f(a)$ 的逆元, 即 $f(a^{-1}) = f(a)^{-1}$;

(3) 若 $a \in G_1$ 的阶是有限的, 则 $f(a)$ 的阶 $o(f(a))$ 一定整除 a 的阶 $o(a)$.

证明 (1) 由于对任意的 $a \in G_1$, 有 $e_1 a = a$, 故

$$f(e_1 a) = f(e_1)f(a) = f(a) = e_2 f(a),$$

① Feit W, Thompson J G. Solvability of groups of odd order. Pacific J. Math., 1963, 13: 775–1029.

因而 $e_2 = f(e_1)$.

(2) 由于对任意的 $a \in G_1$, 有 $f(a^{-1})f(a) = f(a^{-1}a) = f(e_1) = e_2$, 故 $f(a^{-1}) = f(a)^{-1}$.

(3) 由于对任意的 $a \in G_1$, 有 $f(a)^{o(a)} = f(a^{o(a)}) = f(e_1) = e_2$, 故 $f(a)$ 的阶一定整除 a 的阶 $o(a)$. ■

例 1.7.1　设 H 是 G 的正规子群, 则 $\pi : G \to G/H, a \mapsto \bar{a}$ 是一个满同态, 称为 G 到 G/H 的自然同态.

例 1.7.2　令

$$G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} | a \in \mathrm{Z} \right\}.$$

则 G 在矩阵乘法下构成一个群, 映射

$$f : G \to Z, \quad \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mapsto a$$

是一个同构.

例 1.7.3　设 g 是群 G 中某个元素, 映射

$$f : G \to G, a \mapsto g^{-1}ag$$

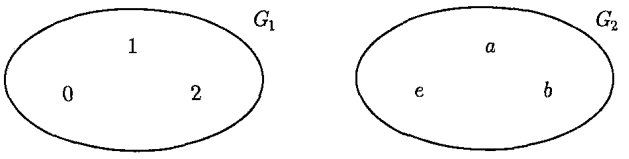
是 G 的一个自同构, 称为**内自同构**(inner automorphism).

设 A, B 都是 n 阶方阵, 若有可逆方阵 P, 使得 $P^{-1}AP = B$, 则 B 是 A 的相似矩阵. 因此当 G 为 n 阶可逆矩阵群 $GL_n(K)$ 时, 内自同构就是矩阵的相似变换.

定义 1.7.3　*如果 f 既是单同态又是满同态, 即是双射, 则 f 称为同构* (isomorphism). *如果两个群 G_1, G_2 之间存在一个同构, 则称这两个群是同构的, 记作 $G_1 \cong G_2$. 群 G 到它自身的一个同构称为自同构* (automorphism).

群的同构概念属于伽罗瓦, 两个同构的群意味着它们有相同的群结构, 因此可以将不同的两个同构群说成是同一个群. 比如说只有一个 2 阶群, 就意味着任何两个 2 阶群是同构的.

在下面的两个群 G_1 和 G_2 中, 表面上来看, 它们的元素不同, 运算也不同, 但它们的代数结构是一样的.



在 G_2 中, 取 $e=1, a=\mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$, $b=\mathrm{e}^{\frac{4\pi \mathrm{i}}{3}}$, 则在乘法下 G_2 是一个乘法群, 而 G_1 是满足 $1+2=0$ 的加法群.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

G_1 的群表

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

G_2 的群表

从上面的群表可以看出, 如果定义映射 $f: G_1 \to G_2$ 为 $f(0)=1$, $f(1)=a$, $f(2)=b$, 则 f 为 G_1 到 G_2 的同构, 从代数结构来讲, G_1 和 G_2 是一样的.

要证明两个群同构, 就需要构造出一个同构映射来, 但有时是比较困难的. 当要判别两个群不同构时, 其实只要找到一个和群有关的性质, 一个群具有该性质, 而另一个群不具有就可以了.

例 1.7.4 试证明有理数加法群 $(\mathbf{Q},+)$ 和非零有理数乘法群 $(\mathbf{Q}^*,\cdot)$ 一定不同构.

证明 反证法. 假设有理数加法群 $(\mathbf{Q},+)$ 和非零有理数乘法群 $(\mathbf{Q}^*,\cdot)$ 同构, f 为同构映射, 则存在 $q\in Q$, 使得 $f(q)=-1$, 故

$$\left[f\left(\frac{q}{2}\right)\right]^2 = f\left(\frac{q}{2}\right) f\left(\frac{q}{2}\right) = f\left(\frac{q}{2}+\frac{q}{2}\right) = f(q) = -1.$$

从而有理数 $f\left(\dfrac{q}{2}\right)$ 的平方为 -1, 矛盾, 所以有理数加法群 $(\mathbf{Q},+)$ 和非零有理数乘法群 $(\mathbf{Q}^*,\cdot)$ 一定不同构. ■

例 1.7.5 由于 $\mathbf{Z}_2$ 和 $\mathbf{Z}_8$ 是交换群, 故可用 $\mathbf{Z}_2\oplus\mathbf{Z}_8$ 来表示 $\{(\overline{m},\overline{n})|\overline{m}\in\mathbf{Z}_2, \overline{n}\in\mathbf{Z}_8\}$ 在加法 $(\overline{m}_1,\overline{n}_1)+(\overline{m}_2,\overline{n}_2)=(\overline{m}_1+\overline{m}_2,\overline{n}_1+\overline{n}_2)$ 下构成的交换群. 虽然 $\mathbf{Z}_2\oplus\mathbf{Z}_8$ 和 $\mathbf{Z}_4\oplus\mathbf{Z}_4$ 都是 16 阶 Abel 群, 但它们不同构, 因为群 $\mathbf{Z}_2\oplus\mathbf{Z}_8$ 具有一个 8 阶元, 而群 $\mathbf{Z}_4\oplus\mathbf{Z}_4$ 没有 8 阶元.

例 1.7.6 设 H 是 G 的一个子群, 则 $i: H\to G, h\mapsto h$ 是一个单同态. 反之, 若 $f: G_1\to G_2$ 是一个单同态, 则 G_1 可以看做 G_2 的一个子群.

3　同态和同构的定理

定理 1.7.1(同态基本定理)　设 $f: G_1 \to G_2$ 是一个群同态, 则

(1) f 的核 $\mathrm{Ker}(f)$ 是 G_1 的正规子群;

(2) 商群 $G_1/\mathrm{Ker}(f)$ 与 f 的像 $\mathrm{Im}(f)$ 同构.

证明　(1) 容易验证 $\mathrm{Ker}(f)$ 是 G_1 的正规子群.

(2) 定义映射 $\varphi: G_1/\mathrm{Ker}(f) \to \mathrm{Im}(f)$, 对任意 $a\mathrm{Ker}(f) \in G_1/\mathrm{Ker}(f)$, 规定 $\varphi(a\mathrm{Ker}(f)) = f(a)$.

先验证 φ 的这个定义是合理的, 即设 $a' \in a\mathrm{Ker}(f)$ 是另一个代表元, 则 $a' = ah, h \in \mathrm{Ker}(f)$. 于是

$$f(a') = f(a)f(h) = f(a)e_2 = f(a).$$

这就证明了 $\varphi(a\mathrm{Ker}(f))$ 与代表元 a 的选取无关, 因此映射 φ 的定义是合理的.

容易验证 φ 是满同态. 设 $a\mathrm{Ker}(f), b\mathrm{Ker}(f) \in G_1/\mathrm{Ker}(f)$ 满足 $f(a) = f(b)$, 则 $f(a^{-1}b) = e_2$. 于是 $a^{-1}b \in \mathrm{Ker}(f)$, 因而 $a\mathrm{Ker}(f) = b\mathrm{Ker}(f)$, 故 φ 是单同态, 所以 $G_1/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. ■

下面例子给出了同态基本定理的应用.

例 1.7.7　任何一个 n 阶循环群同构于商群 $\mathbf{Z}/\mathbf{Z}_n$.

证明　设 G 是一个 n 阶循环群, 以 a 为生成元. 作映射

$$f: \mathbf{Z} \to G, \quad m \mapsto a^m.$$

则 f 是一个满同态, 并且以 $n\mathbf{Z}$ 为核. 由同态基本定理得知

$$\mathbf{Z}/\mathbf{Z}_n \cong G.$$ ■

由上面的例子, 容易知道下面结论成立.

命题 1.7.1　*所有同阶的有限循环群是同构的.*

例 1.7.8　$C[0,1]$ 为 $[0,1]$ 上的所有连续函数在函数加法下构成的交换群, 定义 $C[0,1]$ 到实数 $\mathbf{R}$ 的映射 f, $f: a(t) \mapsto a(0)$, 则容易验证 f 是 $C[0,1]$ 到实数 $\mathbf{R}$ 的群同态, 并且 f 是满的, 因此由同态基本定理可知 $C[0,1]/\mathrm{Ker}(f) \cong \mathbf{R}$.

性质 1.7.2 设 $f: G_1 \to G_2$ 是一个群同态, H_2 是 G_2 的一个子群, 则 $f^{-1}(H_2) = \{a \in G_1 | f(a) \in H_2\}$ 是 G_1 的一个包含 $\mathrm{Ker}(f)$ 的子群.

证明 设 $a, b \in f^{-1}(H_2)$, 则 $f(a), f(b) \in H_2$. 于是 $f(ab^{-1}) = f(a)f(b)^{-1} \in H_2$. 因此 $ab^{-1} \in f^{-1}(H_2)$, 所以 $f^{-1}(H_2)$ 是 G_1 的子群.

设 $a \in \mathrm{Ker}(f)$, 则 $f(a) = e_2 \in H_2$. 故 $a \in f^{-1}(H_2)$, 所以 $\mathrm{Ker}(f) \subseteq f^{-1}(H_2)$. ■

容易想到, 商群的商群会很复杂, 好在下面的同构定理可以使这种复杂性变得简单些.

定理 1.7.2(第一同构定理) 设 H 和 N 都是 G 的正规子群, 且 $H \subseteq N$, 则

$$(G/H)\,/\,(N/H) \cong G/N.$$

证明 由于 H 和 N 都是 G 的正规子群, 且 $H \subseteq N$, 故 H 是 N 的正规子群, 并且 N/H 是 G/H 的正规子群, 因而式子中的所有商群都是有意义的.

令 $\varphi: G \to (G/H)/(N/H)$ 为自然同态 $G \to G/H$ 和 $G/H \to (G/H)/(N/H)$ 的复合, 由于自然同态都是满同态, 故 φ 是一个满同态.

明显地, $N \subseteq \mathrm{Ker}(\varphi)$. 反过来, 若 $g \in \mathrm{Ker}(\varphi)$, 则 $gH \in N/H$, 故存在 $s \in N$, 使得 $gH = sH$, 因而由 $H \subseteq N$ 可得 $g \in N$, 因此 $\mathrm{Ker}(\varphi) \subseteq N$.

所以 $N = \mathrm{Ker}(\varphi)$, 根据同态基本定理可知第一同构定理成立. ■

定理 1.7.3(第二同构定理) 设 H 是 G 的正规子群, K 是 G 的一个子群. 令

$$KH = \{ab | a \in K, b \in H\},$$

则 KH 是 G 的子群, 且

$$KH/H \cong K/K \cap H.$$

证明 (1) 设 $s, t \in KH$, 则 $s = ab, t = cd$, 其中 $a, c \in K, b, d \in H$. 于是

$$st^{-1} = abd^{-1}c^{-1} = (ac^{-1})(cbd^{-1}c^{-1}) \in KH.$$

因此, KH 是 G 的子群.

(2) 容易知道 H 是 KH 的正规子群和 $K \cap H$ 是 K 的正规子群.

(3) 作映射 $\varphi: K \to KH/H, a \mapsto aH$, 则 φ 是一个满同态, 并且以 $K \cap H$ 为核, 因此由同态基本定理可知本定理成立. ■

思考题 1.7.1　一个群有可能与它的真子群同构吗?

可以的. 事实上, 整数加法群 $\mathbf{Z}$ 和它的偶数子群 H 之间存在同构 $\varphi: \mathbf{Z} \to H$, $\varphi(n) = 2n$, 因此整数群 $\mathbf{Z}$ 与它真子群 H 同构.

4　变换群的定义

定义 1.7.4　非空集合 A 的所有可逆变换关于变换的合成所构成的群, 称为 A 的对称群 (symmetric group), 记为 S_A, S_A 的一个子群称为 A 的一个变换群 (transformation group).

容易看出, 当 A 为有限集时, 如 $A = \{1, 2, 3, \cdots, n\}$, 则 S_A 就是前面讨论过的对称群 S_n.

5　Cayley 定理

Cayley 在 1854 年证明了下面的结果, 揭示了变换群与一般群之间的关系.

定理 1.7.4　每一个群都与一个变换群同构.

证明　设 G 是一个群, 则对任意的 $a \in G$, 定义 G 到 G 的变换为

$$f_a: x \to ax, \quad \text{任意 } x \in G,$$

则容易知道 f_a 是 G 到 G 的可逆变换, 因此不难验证 $H = \{f_a | a \in G\}$ 关于变换的合成构成 S_G 的一个子群.

令 $\varphi: a \to f_a$, 则容易知道 φ 是满射, 对于 G 中两个不同的元素 a 和 b, 有 $f_a(e)$ 与 $f_b(e)$ 不相等, 因此 f_a 与 f_b 不相等, 从而 φ 是单射, 故 φ 为 G 到 H 的一一对应.

由于 $\varphi(ab) = f_{ab} = f_a f_b = \varphi(a)\varphi(b)$, 故是 G 到 H 的同构, 所以任意一个群都与一个变换群同构. ■

例 1.7.9　若 $G = \{1, \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}, \mathrm{e}^{\frac{4\pi \mathrm{i}}{3}}\}$, 则 G 在乘法下为群, 并且

$$f_1: x \to x,$$

$$f_{e^{\frac{2\pi i}{3}}}: x \to e^{\frac{2\pi i}{3}} x,$$
$$f_{e^{\frac{4\pi i}{3}}}: x \to e^{\frac{4\pi i}{3}} x,$$

因此

$$f_1 = \begin{pmatrix} 1 & e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} \end{pmatrix},$$
$$f_{e^{\frac{2\pi i}{3}}} = \begin{pmatrix} 1 & e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} \\ e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} & 1 \end{pmatrix},$$
$$f_{e^{\frac{4\pi i}{3}}} = \begin{pmatrix} 1 & e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} \\ e^{\frac{4\pi i}{3}} & 1 & e^{\frac{2\pi i}{3}} \end{pmatrix}.$$

如用循环来表示, 则

$$f_1 = (1), \quad f_{e^{\frac{2\pi i}{3}}} = (123), \quad f_{e^{\frac{4\pi i}{3}}} = (132),$$

因此容易知道 G 与 S_3 的子群 $H = \{(1), (123), (132)\}$ 同构.

推论 1.7.1 *若 G 是 n 阶有限群, 则 G 与 S_n 的一个子群同构.*

思考题 1.7.2 *对任何给定的正整数 n, 互不同构的 n 阶群一定只有有限个吗?*

事实上, 由于任何 n 阶群都与 n 次对称群 S_n 的一个子群同构, 但 S_n 是 $n!$ 阶有限群, 它只能有有限个子群, 故互不同构的 n 阶群只有有限个.

1.8 群的直积

群的直积是研究群的主要方法之一, 利用直积可以将较大的群分解成一些较小的子群的乘积, 从而可能把研究较复杂的群简化为研究较简单的群. 利用直积, 还可以从已知的群中构造出新的群.

1 群的内直积

定义 1.8.1 *设 G 是一个群, $N_i (i = 1, 2, \cdots, n)$ 是 G 的 n 个正规子群且适合下列条件:*

(1) $G = N_1 N_2 \cdots N_n$;

(2) $N_i \cap N_1 \cdots N_{i-1}N_{i+1} \cdots N_n = \{e\}$ 对一切 $i = 1, 2, \cdots, n$ 成立;

则称 G 是 $N_i (i = 1, 2, \cdots, n)$ 的内直积.

定理 1.8.1　设 $N_i (i = 1, 2, \cdots, n)$ 是群 G 的正规子群, 则 G 是 $N_i (i = 1, 2, \cdots, n)$ 的内直积的充要条件是:

(1) $G = N_1 N_2 \cdots N_n$;

(2) G 中元素用 N_i 中元的乘积表示唯一, 即若

$$g = g_1 g_2 \cdots g_n = h_1 h_2 \cdots h_n,$$

则必有 $g_i = h_i (i = 1, 2, \cdots, n)$.

证明　设 G 是 $N_i (i = 1, 2, \cdots, n)$ 的内直积, 明显地只需证明 (2) 成立.

若 $g_i \in N_i, g_j \in N_j, i \neq j$, 由于 $N_i \cap N_j \subseteq N_i \cap N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n = \{e\}$, 故 $N_i \cap N_j = \{e\}$. 由 N_j 是群 G 的正规子群可知 $g_i g_j g_i^{-1} g_j^{-1} = (g_i g_j g_i^{-1}) g_j^{-1} \in N_j$. 同理可证 $g_i g_j g_i^{-1} g_j^{-1} = g_i (g_j g_i^{-1} g_j^{-1}) \in N_i$, 故 $g_i g_j g_i^{-1} g_j^{-1} = e$, 从而 $g_i g_j = g_j g_i$.

如果 $g = g_1 g_2 \cdots g_n = h_1 h_2 \cdots h_n (g_i, h_i \in N_i)$, 那么

$$\begin{aligned} h_1^{-1} g_1 =& h_2 \cdots h_n g_n^{-1} g_{n-1}^{-1} \cdots g_2^{-1} \\ =& h_2 \cdots h_{n-1} (h_n g_n^{-1}) g_{n-1}^{-1} \cdots g_2^{-1} \\ =& h_2 \cdots h_{n-1} g_{n-1}^{-1} (h_n g_n^{-1}) g_{n-2}^{-1} \cdots g_2^{-1} \\ & \cdots\cdots \\ =& (h_2 g_2^{-1})(h_3 g_3^{-1}) \cdots (h_n g_n^{-1}) \\ & \in N_2 N_3 \cdots N_n. \end{aligned}$$

因此 $h_1^{-1} g_1 \in N_1 \cap N_2 N_3 \cdots N_n = \{e\}$, 即 $h_1 = g_1$. 从而由 $g = g_1 g_2 \cdots g_n = h_1 h_2 \cdots h_n$ 可得, $g_2 \cdots g_n = h_2 \cdots h_n$. 利用同样方法可证得 $g_2 = h_2, \cdots, g_n = h_n$.

反过来, 如果 (1)、(2) 成立, 要证 $N_i \cap N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n = \{e\}$ 对 $i = 1, 2, \cdots, n$ 成立, 令 $a \in N_i \cap N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n$, 则

$$a = g_i = g_1 \cdots g_{i-1} g_{i+1} \cdots g_n,$$

即

$$e \cdots e g_i e \cdots e = g_1 \cdots g_{i-1} e g_{i+1} \cdots g_n$$

由表示唯一即得 $g_i = e, a = e$, 所以 $N_i \cap N_1N_2\cdots N_{i-1}N_{i+1}\cdots N_n = \{e\}$. ■

推论 1.8.1 设 $N_i(i = 1,2,\cdots,n)$ 是群 G 的正规子群, 则 G 是 $N_i(i = 1,2,\cdots,n)$ 的内直积的充要条件是:

(1) $G = N_1N_2\cdots N_n$;

(2) 若 $g_1g_2\cdots g_n = e, g_i \in N_i$, 则 $g_i = e(i = 1,2,\cdots,n)$.

证明 明显地, 只需证明 G 中元素用 N_i 中元的乘积表示唯一.

若 $a \in N_i \cap N_j(i \neq j)$, 则 $a = a_i = a_j, a_i \in N_i, a_j \in N_j$, 故 $a_ia_j^{-1} = e, a_i = e, a_j = e$, 从而 $N_i \cap N_j = \{e\}(i \neq j)$.

由 $N_i(i = 1,2,\cdots,n)$ 是群 G 的正规子群可证, 若 $b_i \in N_i, b_j \in N_j, (i \neq j)$, 则 $b_ib_j = b_jb_i$. 如果 $g = g_1g_2\cdots g_n = h_1h_2\cdots h_n$, $g_i, h_i \in N_i$, 则由于 $b_ib_j = b_jb_i$ 对一切 $b_i \in N_i, b_j \in N_j, (i \neq j)$ 都成立, 故

$$g_1h_1^{-1}g_2h_2^{-1}\cdots g_nh_n^{-1} = (g_1g_2\cdots g_n)(h_1h_2\cdots h_n)^{-1} = e.$$

因而 $g_ih_i^{-1} = e, g_i = h_i$, 所以推论成立.

2 群的外直积

定义 1.8.2 设 G 是群, $G_i(i = 1,2,\cdots,n)$ 是 n 个群, $G = G_1 \times G_2 \times \cdots \times G_n$, 定义 G 中的乘法:

$$(g_1, g_2, \cdots, g_n)(h_1, h_2, \cdots, h_n) = (g_1h_1, g_2h_2, \cdots, g_nh_n),$$

则 G 在该乘法下构成的群称为是 $G_i(i = 1,2,\cdots,n)$ 的外直积.

内直积和外直积在同构的意义下是一致的.

定理 1.8.2 设群 G 是它的正规子群 $N_i(i = 1,2,\cdots,n)$ 的内直积, 又 $T = N_1 \times N_2 \times \cdots \times N_n$ 是 $N_i(i = 1,2,\cdots,n)$ 的外直积, 则 G 与 T 同构.

证明 令 $\varphi : T \to G$ 为

$$\varphi(g_1, g_2, \cdots, g_n) = g_1g_2\cdots g_n,$$

则 φ 是满射.

由于

$$\begin{aligned}&\varphi((g_1,g_2,\cdots,g_n)(h_1,h_2,\cdots,h_n))\\=&\varphi(g_1h_1,g_2h_2,\cdots,g_nh_n)\\=&g_1h_1\cdot g_2h_2\cdots g_nh_n\\=&g_1g_2\cdots g_nh_1h_2\cdots h_n\\=&\varphi((g_1,g_2,\cdots,g_n))\varphi((h_1,h_2,\cdots,h_n)),\end{aligned}$$

故 φ 是群同态.

若 $\varphi(g_1,g_2,\cdots,g_n)=e$, 则 $g_1g_2\cdots g_n=e$, 故 $g_i=e$, 因而 φ 是单射, 所以 G 与 T 同构. ■

基于上面的结论, 有时不再区分外直积与内直积, 统称为群的直积.

例 1.8.1　设 G 是 pq 阶循环群且 p 和 q 是互素的正整数, 试证明 G 可分解为 p 阶循环子群与 q 阶循环子群的直积.

证明　设 $G=<a>$, 由于 p 和 q 互素, 故存在整数 s 和 t 使得 $sp+tq=1$, 于是

$$a=a^{ps}a^{qt}=(a^p)^s(a^q)^t.$$

令 $G_1=<a^p>$, $G_2=<a^q>$, 则 $G=G_1G_2$. 若 $b\in G_1\cap G_2$, 则 $o(b)$ 整除 $|G_1\cap G_2|$, 从而 $o(b)|p, o(b)|q$. 但 $(p,q)=1$, 故 $o(b)=1$, 从而 $b=e$, 因此 $G=G_1\times G_2$. 明显地, a^p 周期为 q, a^q 的周期为 p, 所以 G 可分解为 p 阶循环子群 G_1 与 q 阶循环子群 G_2 的直积. ■

例 1.8.2　六阶循环群是二阶循环群和三阶循环群的直积.

证明　令 $G=\mathbf{Z}/6\mathbf{Z}$, 则 G 有二阶子群 $H_1=\{\bar{0},\bar{3}\}$ 和三阶子群 $H_2=\{\bar{0},\bar{2},\bar{4}\}$, 并且 H_1 和 H_2 满足定理 1.8.1 的条件, 所以, G 是二阶循环群 H_1 和三阶循环群 H_2 的内直积. ■

例 1.8.3　试证明无限循环群 G 不同构于它的两个非平凡群的直积.

证明　反证法. 假设无限循环群 $G=<a>$, 它有两个非平凡子群 $H=<a^m>$ 和 $K=<a^n>$, 使得 G 是它们的内直积, 则

$$H\cap K=\{e\}.$$

但这与 $a^{mn} \in H \cap K$ 矛盾, 所以由反证法原理可知, G 不同构于它的两个非平凡群的直积. ■

1.9 拓 扑 群

拓扑群就是引进了拓扑的群, 并且群的乘法和求逆运算关于它的拓扑都是连续的. Schreier 在 1925 年和 Leja 在 1927 年用略微有点不同的术语定义了拓扑群, 不过 Leja 的更接近现在的定义. Schreier 还证明了若 H 是拓扑群 G 的闭正规子群, 则 G/H 是拓扑群. Hausdorff 发现对于一个给定的非空集合, 可以用某种方式来确定某些子集为开集, 然后利用开集就可以建立闭集、闭包和序列收敛等概念, Hausdorff 利用这些概念建立了拓扑空间理论.

1 拓扑的定义

定义 1.9.1 设 G 是一个非空集合, τ 是 G 的一族子集, 若 τ 满足下面的三个公理, 则称 (G,τ) 是拓扑空间.

(1) $\varnothing \in \tau$, $G \in \tau$;

(2) τ 中任意个集合的并集属于 τ;

(3) τ 中任意有限个集合的交集属于 τ.

此时称 τ 中每一个集合为开集, 称 τ 为拓扑. 若 H 的补集 H^C 是开集, 则称 H 为闭集.

例 1.9.1 设 G 是一个非空集合, τ 为 G 的子集的全体, 则 (G,τ) 是一个拓扑空间, 此时称 τ 为 G 的离散拓扑. 此时, 对任意 $a \in G$, $\{a\}$ 都是开集.

例 1.9.2 设 $G = \{e, a, b\}$, $\tau = \{\varnothing, G, \{e\}, \{e, a\}, \{e, b\}\}$, 则 (G,τ) 为一拓扑空间, 并且在 (G,τ) 中, 对含有 a 点和含有 b 点的任意开集 U_a 和 U_b, 都有 $U_a \cap U_b = \varnothing$.

定义 1.9.2 拓扑空间 (G,τ) 称为 Hausdorff 空间, 若对于 G 中的任意 a, b, $a \neq b$, 存在两个开集 U_a 和 U_b, 使得 $a \in U_a$, $b \in U_b$, 且 $U_a \cap U_b = \varnothing$.

2　拓扑群的定义

拓扑群是群与拓扑空间的结合, 所谓结合, 就是群的运算与拓扑空间的结构相容.

定义 1.9.3　*集合 G 称为拓扑群, 如果*

(1) *G 是群.*

(2) *G 是拓扑空间.*

(3) *对任意的 $a,b\in G$, 群的运算 $(a,b)\to ab^{-1}$ 是 $G\times G\to G$ 的连续映射.*

条件 (3) 表示了群的运算与拓扑结构的相容性, 也常称为相容条件.

思考题 1.9.1　*在任意给定的群 G 上, 是否可以定义拓扑, 使得 G 成为一个拓扑群?*

例 1.9.3　在任意给定的群 G 上, 定义离散的拓扑 τ 成为一个离散的拓扑空间. 显然, 群的运算 $(a,b)\to ab^{-1}$ 是连续的, 因而群 G 在离散拓扑 τ 下是拓扑群. 这就是说, 任意一个群都可以看做一个离散的拓扑群.

例 1.9.4　全体实数 $\mathbf{R}$ 对加法构成群, 显然群的运算对 $\mathbf{R}$ 上的通常的拓扑相容, 因而是拓扑群.

定义 1.9.4　*作为群的子群与其诱导拓扑构成拓扑群, 并称为拓扑子群. 也就是说, 它既是子群又是拓扑子空间.*

例 1.9.5　$\mathbf{R}$ 中的全体有理数群 $\mathbf{Q}$ 是 $\mathbf{R}$ 的子群. $\mathbf{Q}$ 作为拓扑空间 $\mathbf{R}$ 的子集对其诱导拓扑构成一拓扑空间, 即 $\mathbf{R}$ 的拓扑子空间. 显然, 有理数群 $\mathbf{Q}$ 的运算是连续的, 因而 $\mathbf{Q}$ 也是拓扑群, 它是 $\mathbf{R}$ 的拓扑子群.

思考题 1.9.2　*拓扑群的定义中的相容条件 (3) 能不能用 $(a,b)\to ab$ 是连续的来代替呢?*

例 1.9.6　在实数加法群 $\mathbf{R}$ 上规定如下的拓扑. 对 $\mathbf{R}$ 上任意一点 a, 对于任意的正实数 ε, 定义半开区间 $[a,a+\varepsilon)$ 为 a 的开集, 记这样定义的开集全体生成的拓扑为 τ. 容易知道对于 $a<b$, 开区间 (a,b), 左闭右开的区间 $[a,b)$ 和 $(-\infty,+\infty)$ 都是拓扑空间 $(\mathbf{R},\tau)$ 的开集. 但是对于 $a<b$, 闭区间 $[a,b]$ 和左开右闭的区间 $(a,b]$ 都不是拓扑空间 $(\mathbf{R},\tau)$ 的开集. 对该拓扑 τ, 不难验证, 实数加法群 $\mathbf{R}$ 的加法运算是连续的, 但减法运算不连续. 因此, 实数加法群 $\mathbf{R}$ 在拓扑 τ 下不是拓扑群.

3 拓扑群的性质

容易看出下面定理成立.

定理 1.9.1 *若 G 是群且是拓扑空间, 则 G 中群的运算和拓扑结构相容的充分必要条件是 $G\times G\to G$ 的映射 $(a,b)\to ab$ 和 $G\to G$ 的映射 $a\to a^{-1}$ 都是连续的.*

定义 1.9.5 *若 G 是拓扑群, 则 $G\to G$ 的映射 $\varphi: a\to a^{-1}$ 是连续的, 称 φ 为 G 的逆射.*

因为群 G 中任意元素的逆元素都存在, 所以 φ 是满映射.

定理 1.9.2 *若 G 是拓扑群, 则逆射 φ 是拓扑群 G 上的同胚, 即 φ 是双射, φ 和 φ^{-1} 都是群 G 到群 G 的同构映射, 并且都是拓扑连续的.*

若拓扑空间 (G,τ) 的任意一个点 a 与不包含这个点的闭集 H, 一定存在包含 a 的开集 U_a 和包含 H 的开集 U_H, 使得 $U_a\cap U_H=\varnothing$, 则称拓扑空间 (G,τ) 为正则的.

定理 1.9.3 *拓扑群 G 作为拓扑空间是正则的.*

定理 1.9.4 *若拓扑群 G 的子群 H 是开集, 则 H 一定是闭集.*

证明 设 H 是拓扑群 G 的一个开子群, 由于左乘是同胚, 故对 G 中的任意元意 a, aH 都是开集.

若 $a\notin H$, 则 aH 与 H 不相交. 假若不然, 即 $aH\cap H\neq\varnothing$, 必有 $b\in aH\cap H$, 从而必有 $h\in H$ 使 $b=ah$. 又因为 H 是子群, 故 $a=bh^{-1}\in H$, 与 $a\notin H$ 的假设矛盾. 因而 $\bigcup\limits_{a\notin H}aH$ 是开集, 且是 H 的余集, 所以 H 是闭集. ■

若 (G,τ) 是拓扑空间, H 是 G 的子集, 则称包含 H 的最小闭集为 H 的闭包, 记为 $\bar{H}$.

定理 1.9.5 *拓扑群 (G,τ) 的子群 H 的闭包 $\overline{H}$ 也是子群.*

类似地, 还可证下面结论成立.

定理 1.9.6 *若 H 是 G 的正规子群, 则 H 的闭包 $\overline{H}$ 也是 G 的正规子群.*

定义 1.9.6 *拓扑空间 (G,τ) 称为连通的, 如果 G 不能表为两个非空, 不相交的开集之并. 反之, 则称 G 是不连通的.*

显然, 一个拓扑空间是连通的当且仅当它没有非平凡的既开又闭的子集.

定理 1.9.7　*若 G 是连通拓扑群, 则它没有真开子群.*

4　拓扑群研究概况

在拓扑群中研究得最多的是局部欧氏群. 当拓扑群 G 的某一点有邻域同胚于欧氏空间的开集, 则 G 称为局部欧氏群. Hilbert 第 5 问题为是否所有的局部欧氏群都是李群. 1933 年 von Neumann 在紧群的情况下解决了 Hilbert 第 5 问题①, 1934 年 Pontryagin 解决了局部紧 Abel 群的情形. Hilbert 第 5 问题最终的彻底解决为 Gleason, Montgomery 和 Zippin 在 1952 年获得.

习　题　一

1.1　试验证形如

$$A=\begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}$$

的矩阵在矩阵乘法下是一个群.

1.2　设 $G=\{f(t)|f(t)$ 为 $[0,1]$ 的严格单调递增的连续函数, 并且满足 $f(0)=0, f(1)=1\}$, 对于 $f,g\in G$, 定义乘法 $f\cdot g(t)=f(g(t))$, 试证明 G 是一个群.

1.3　试证明有限群 G 中的每个元素的阶一定是有限的.

1.4　设 G 是非交换群, 试证明一定存在 $a\in G$, 使得 $a^2=e$ 不成立.

1.5　设 G 是阶大于 2 的非交换群, 试证明一定存在 $a,b\in G$, a 和 b 都不是单位元, 并且 $ab=ba$.

1.6　若群 G 是有限群, $a,b\in G$, 试证明 ab 和 ba 的阶是一样的. 另外, 此时 abc, bca 和 cab 的阶是一样的吗?

1.7　若群 G 中的元 c 的阶为 mn, 并且 m 与 n 互素, 试证明一定存在 $a,b\in G$, 使得 a 的阶为 m, b 的阶为 n, 并且 $c=ab$.

1.8　若 H 是交换群 G 中所有的有限阶的元素, 试证明 H 是 G 的一个子群. 如果 G 是非交换群, 那么 H 还是不是 G 的一个子群?

① von Neumann J. Die einführung analytischer parameter in topologischen gruppen. Ann. of Math., 1933, 34: 170–190.

1.9 设 H 和 K 是群 G 两个非空子群, 若 H 的阶与 K 的阶的和大于群 G 的阶, 试证明一定有 $G = HK$.

1.10 试证明任意一个群 G 都不可能是它的两个真子群 H 和 K 的并集.

1.11 所有 2×2 可逆矩阵 $GL(2, R)$ 全体在矩阵的相乘的乘法下构成非交换群, 若 $a = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$, 试求 a 的中心 $C(a)$.

1.12 试证明循环群 $G = < a >$ 的子群 H 一定是循环群.

1.13 设 G 是 n 阶循环群, 若 m 整除 n, 试证明存在且只存在一个阶为 m 的子群.

1.14 设 G 是一个群, $a, b \in G$, 若 a 的阶为素数 p, 并且 $a \notin < b >$, 试证明 $< a >$ 与 $< b >$ 的交一定是 $\{e\}$.

1.15 设 G 是群, 试证明下列条件是等价的:

(1) G 是 Abel 群;

(2) 对于所有的 $a, b \in G$, 都有 $(ab)^2 = a^2b^2$;

(3) 对于所有的 $a, b \in G$, 都有 $(ab)^{-1} = a^{-1}b^{-1}$.

1.16 设 G 是所有有理数上的 2×2 满秩矩阵全体在矩阵的相乘的乘法下构成的非交换群, 试找出阶为无限的 a 和阶为有限的 b, 使得 ab 的阶是有限的.

1.17 4 阶的 Abel 群是否一定为循环群.

1.18 试给出一个群 G, 使得 G 可以写成它的 3 个真子群的并集.

1.19 试证明 4 阶群 G 一定是 Abel 群.

1.20 若群 G 的阶是奇数, 试证明对任意的 $a \in G$, 存在唯一的 $b \in G$, 使得 $a = b^2$.

1.21 试给出三次对称群 S_3 的所有真子群.

1.22 设

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}; \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 1 & 5 & 2 & 3 & 7 \end{pmatrix}.$$

(1) 求 σ_1^{-1}, σ_1^{-1} 的阶;

(2) 求 $\sigma_2\sigma_1\sigma_2^{-1}$.

1.23　设 $\sigma_1=(327)(26)(14)$, $\sigma_2=(134)(57)$, 试求 $\sigma_2\sigma_1\sigma_2^{-1}$ 和 $\sigma_2^{-1}\sigma_1\sigma_2$.

1.24　试给出 S_4 的一个正规子群.

1.25　设 H 和 K 都是群 G 的正规子群, 若 $H\cap K=\{e\}$, 试证明对任意 $a\in H, b\in K$, 都有 $ab=ba$.

1.26　设 H 和 K 分别是群 G 的 m 与 n 阶子群, 若 m 与 n 互素, 试证明 $H\cap K=\{e\}$.

1.27　设 G 是非交换的有限群, H 是 G 的中心, 试证明 H 的阶一定小于等于 G 的阶的四分之一.

1.28　设 H, K 是 G 的子群, 并且 H 是 G 的正规子群, 试证明 HK 是 G 的子群.

1.29　试给出四元数群的所有真子群, 并且给出证明.

1.30　设 n 是奇数, G 是阶为 $2n$ 的有限 Abel 群, 试证明 G 最多只有一个二阶子群.

1.31　试证明 G 是 Abel 群的充要条件为 $f: a\to a^{-1}$ 是群 G 的自同构.

1.32　试证明单群的同态象是单群或单位元群.

1.33　设 f 是群 G_1 到群 G_2 的同态, 试证明对于任意 $a\in G_1$, 有 $f^{-1}(f(a))=a\mathrm{Ker}(f)$.

1.34　设群 G_1 和群 G_2 是阶分别为 m, $n(m>n)$ 的循环群, 试证明 n 整除 m 的充要条件为存在 $f: G_1\to G_2$ 为群 G_1 到群 G_2 的满同态.

1.35　设 H 是群 G 的正规子群, H 是 G 的极大正规子群是指如果 K 是正规子群, 并且 $H\subset K\subset G$, 则一定有 $H=K$ 或 $K=G$, 试证明 H 是 G 的极大正规子群的充要条件为 G/H 是单群.

1.36　设 H 是群 G 的正规子群, $[G:H]=m, |H|=n$, 并且 m, n 是互素的, 试证明 H 是 G 唯一的阶为 n 的子群.

1.37 设 G_1 和 G_2 群 G 的两个正规子群, 且 G 是 G_1 和 G_2 的内直积, 试证明 $G/G_1 \cong G_2, G/G_2 \cong G_1$.

1.38 设 G_1 和 G_2 是两个群, 试证明 $G_1 \times G_2 \cong G_2 \times G_1$.

1.39 设 H 为拓扑群 G 的一个正规子群, 在商群 G/H 中定义开集为: 在自然同态映射 $\varphi: G \to G/H$ 下, 若 G/H 的一个子集 K 的原像 $\varphi^{-1}(K)$ 是拓扑群 G 中的开集, 则定义 K 为 G/H 的开集, 试证明 G/H 在该拓扑下是一个拓扑群.

1.40 试证明 S_3 的所有真子群都是交换群, 即 S_3 是内交换群.

N. H. Abel(阿贝尔)1802 年 8 月出生于挪威的一个农村, 他很早就显示了数学才华. 16 岁那年, 他遇到了一个能赏识其才能的老师霍姆伯 (Holmboe), 霍姆伯介绍他阅读牛顿、欧拉、拉格朗日、高斯的著作. 大师们创造性的方法和成果, 开阔了阿贝尔的视野, 使他很快就开始了数学研究. 他成功地证明了用根式解一般五次方程是不可能的, 他还研究了更广的一类代数方程, 后人发现这是具有交换的伽罗瓦群的方程. 为了纪念他, 若尔当 (Jordan) 将交换群称为阿贝尔群. 阿贝尔还研究过无穷级数, 得到了一些判别准则以及关于幂级数求和的定理. 这些工作使他成为分析学严格化的推动者. 阿贝尔和雅可比是公认的椭圆函数论的奠基者. 阿贝尔发现了椭圆函数的加法定理、双周期性、并引进了椭圆积分的反演. 2001 年挪威政府宣布创设阿贝尔奖, 以纪念他诞生 200 周年.

瑞士数学家 Gosta Mittag-Leffler 用这样的语言来描述阿贝尔的数学成就: “阿贝尔的最好作品真的是一组高尚优美的抒情诗 …… 在平庸的生活之上升华, 从心灵深处直接发生光彩, 非普通语言文字所能描绘, 超越了任何诗人.”

学习指导

基本要求

1. 熟练掌握半群、群和子群的定义及其性质.

2. 半群 G 是群的充要条件为对任意 $a, b \in G$, 方程 $ax = b$ 和 $ya = b$ 在 G 中有解.

3. 在群 G 中, 若 $o(a)=n$, 则关于 a 的阶, 有下面的一些性质.

(1) $a^m=e$ 的充要条件为 $n|m$.

(2) $o(a^k)=\dfrac{n}{(k,n)}$.

(3) $o(a)=n=st$ 时, 有 $o(a^s)=t$.

(4) $a,b\in G$, 若 $o(a)$ 与 $o(b)$ 互素, 并且 $ab=ba$, 则 $o(ab)=o(a)o(b)$.

4. 由于置换群是群论中经常使用的重要例子, 故要熟悉它的性质和结构.

5. 正规子群是群论的重要概念, 一定要熟练掌握它的性质.

6. Lagrange 定理是一个很有用的重要定理, 但要注意该定理反过来是不一定成立的.

7. 拓扑群部分只需初步了解群与拓扑的联系.

释疑解难

1. 一个群只要有两个元素不能交换, 就称它是非交换群. 存不存在一个群, 它的任意连个元素都是不可交换的呢? 这是不可能的, 因为单位元总是可以跟其他元素交换.

2. 在群 G 中, 元素 a 和 b 的阶一般决定不了乘积 ab 的阶.

3. 在群 G 中, 元素 a 的阶可以决定 a^k 的阶.

(1) 若 a 的阶是无穷, 则当 k 为非零整数时, a^k 的阶也是无穷.

(2) 若 a 的阶是有限的, $o(a)=n$, 则 $o(a^k)=\dfrac{n}{(k,n)}$.

(3) 由于利用元素的阶对群进行分类是研究群的重要方法之一, 故对于元素的阶, 要熟练掌握相关的性质.

4. 群 G 的非空子集 H 构成子群的等价条件为 $HH^{-1}=H$.

5. 群 G 的两个子群 H 和 K 的乘积 HK 是 G 的子群的充要条件为 $HK=KH$. 但要注意的是 $HK=KH$, 并不意味着对任意 $h\in H,k\in K$, 一定有 $hk=kh$. 例

如在四元数群 G 中, 取 $H=\{1,-1,i,-i\}$, $K=\{1,-1,j,-j\}$, 则它们都是 G 的子群, 并且 $HK=KH=G$, 但明显地, 对于 $i\in H, j\in K$, 有 $ij\neq ji$.

6. 群 G 两个陪集的乘积不一定是群 G 一个陪集. 例如对称群 S_3 的子群 $H=\{e,(12)\}$, eH 和 $(13)H$ 是两个左陪集, 但 $eH\cdot(13)H=\{(13),(23),(123),(132)\}$ 不是左陪集.

7. 群 G 不可能是它的两个真子能的并集. 但一个群可能是它的三个或四个真子群的并集. 实际上, 对群 $K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$, 取

$$H_1=\{(1),(12)(34)\},\quad H_2=\{(1),(13)(24)\},\quad H_3=\{(1),(14)(23)\}.$$

则它们都是 K_4 的真子群, 并且 $K_4=H_1\cup H_2\cup H_3$.

另外, 对于对称群 $S_3=\{(1),(12),(13),(23),(123),(132)\}$, 取

$$H_1=\{(1),(12)\}, H_2=\{(1),(13)\}, H_3=\{(1),(23)\}, H_4=\{(1),(123),(132)\},$$

则它们都是 K_4 的真子群, 并且 $S_3=H_1\cup H_2\cup H_3\cup H_4$.

8. 按照群的同构可以将群进行分类, 下面是阶小于等于 7 不同构的群.

2 阶群	Z_2	3 阶群	Z_3
4 阶群	Z_4, $Z_2\oplus Z_2$	5 阶群	Z_5
6 阶群	Z_6, S_3	7 阶群	Z_7

9. 群直积有着重要的意义, 利用直积, 可以由已知的群构造出新的群. 更重要的是, 如果一个群比较复杂, 但可以分解成某些子群的直积, 那么只要将每个子群研究清楚了, 群 G 的性质和结构也就很清楚了.

解题技巧

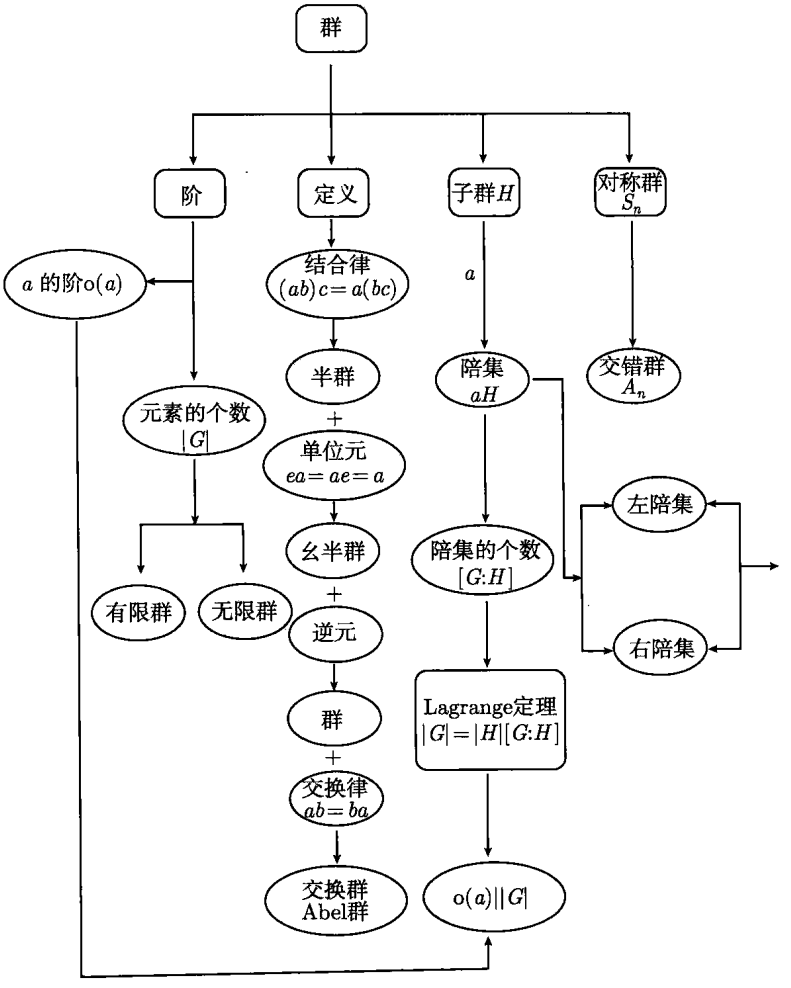
1. 利用 Lagrange 定理解题, 特别要注意对任意 $a\in G$, 有 $o(a)||G|$.

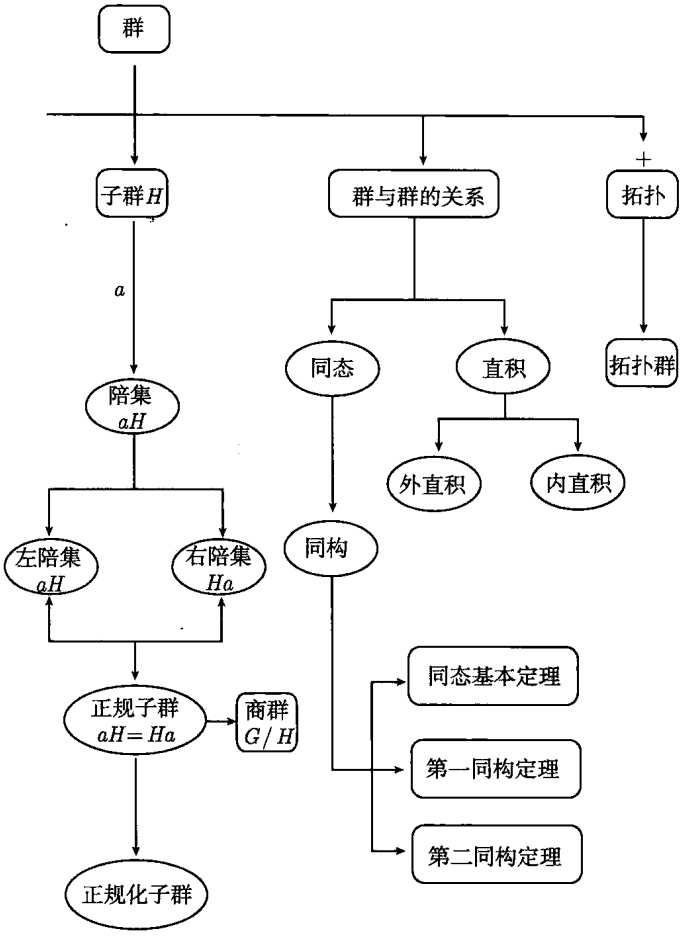
2. 求对称群 S_n 中置换的逆和判断置换的奇偶性.

3. 利用正规子群的性质来证明题目.

4. 证明两个群不同构的技巧.

知识点联系图


群
阶
定义
子群H
对称群S_n
a 的阶o(a)
结合律
$(ab)c=a(bc)$
a
半群
+
单位元
$ea=ae=a$
幺半群
+
逆元
群
+
交换律
$ab=ba$
交换群
Abel群
元素的个数
$|G|$
有限群
无限群
陪集
aH
陪集的个数
$[G:H]$
Lagrange定理
$|G|=|H|[G:H]$
o(a)||G|
交错群
A_n
左陪集
右陪集


群
子群H
群与群的关系
拓扑
a
同态
直积
拓扑群
陪集
aH
外直积
内直积
左陪集
aH
右陪集
Ha
同构
正规子群
aH=Ha
商群
G/H
同态基本定理
第一同构定理
第二同构定理
正规化子群

第2章 环 和 域

在我看来, 一个人如果要在数学上有所进步, 他必须向大师们学习, 而不应向徒弟们学习.

Abel(1802—1829, 挪威数学家)

David Hilbert(1862—1943)

集合中常常同时有几种运算, 并且这些运算互相有一定的关系. 本章将讨论有两个代数运算的代数体系 —— 环和域. 先从比较广泛的环开始, 因为环论中的概念、方法都与群论的概念、方法比较接近. 环的概念, 虽然最初是 Dedekind 在研究代数时引入的, 不过他称之为序 (order), 环这个术语来源于 Hilbert(1897).

Wedderburn 在 1907 年发表的论文中, 研究了结合代数, 而这种代数就是环.

环和理想的系统理论是 Noether 建立的, 她的工作被看做抽象代数学形成的标志.

Richard Dedekind(1831—1916)

2.1 基本概念

1896 年 Hilbert 向德国数学会递交了代数数论的经典报告 "代数数域理论"(*Die Theorie der algebraischen Zahlkrper*), 他在文中首次引入了环的定义, 并将环作为一个独立的概念来加以研究, 但他定义的环是针对数域的数环, 而不是抽象的环.

1 环的定义

在算术中, 若在整数集上只考虑加法、减法和乘法, 则容易知道这些运算满足下面的结合律和分配律.

定义 2.1.1 *设 R 是一个非空集合, 如果在 R 中有两种二元运算 $+$, $\cdot$ 满足以下条件:*

(1) *R 是加法 Abel 群和乘法半群;*

(2) *$a\cdot(b\cdot c)=(a\cdot b)\cdot c$ 对任何 a, b, $c\in R$ 成立;*

(3) *$(a+b)\cdot c=a\cdot c+b\cdot c$ 和 $a\cdot(b+c)=a\cdot b+a\cdot c$ 对任何 $a,b,c\in R$ 成立;*

(4) *存在 $e\in R$, 使 $e\cdot a=a\cdot e=a$ 对任何 $a\in R$ 成立, e 称为 R 中的单位元 (或幺元).*

则称 R 为一个环 (ring).

环的第一个公理化定义是 Fraenkel 在 1914 年给出的, 1921 年 Noether 在论文 Ideal theory in rings 中给出了交换环的公理化定义.

例 2.1.1 全体整数在加法和乘法下构成一个环, 称为整数环, 记为 $\mathbf{Z}$. 全体偶数在加法和乘法下满足环的分配律和结合律, 但它没有单位元, 因此全体偶数不构成一个环. 容易知道, 有理数集 $\mathbf{Q}$、实数集 $\mathbf{R}$、复数集 $\mathbf{C}$ 在通常的加法和乘法下都构成环, 分别称为理数环、实数环和复数环.

例 2.1.2 若 n 是大于 1 的正整数, 则 $\mathbf{Z}_n=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{n-1}\}$ 在剩余类的加法和乘法下构成环, 称为模 n 剩余类环 (residue class ring).

定义 2.1.2 *在环 R 中, 如果 $a\cdot b=b\cdot a$ 对任何 $a,b\in R$ 成立, 则称环 R 为交换环* (commutative ring), *否则就称为非交换环* (non-commutative ring).

一般地, 环中的乘法运算 $a \cdot b$ 常常记成 ab, 加法的零元素和乘法的单位元在不会引起混淆时按习惯分别记作 0 和 1.

命题 2.1.1　设 R 是只含一个元 a 的集合, 若定义 $a+a=a$, $a \cdot a=a$, 则 R 是环, 并且零元素和单位元都是 a, 即 $0=1=a$. 这样的环称为零环, 记作 0.

例 2.1.3　实数域上的所有 $n \times n$ 矩阵 $M_n(\mathbf{R})$ 在矩阵的加法和乘法下构成一个环, 明显地, $n \geqslant 2$ 时, 这个环是非交换的. 如在 $M_2(\mathbf{R})$ 中, 有

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

例 2.1.4　任意一个数域 K 上的多项式全体 $K[x]$ 在通常的加法和乘法下构成一个交换环, 称为**数域K上的多项式环**.

例 2.1.5　设 $C[0,1]$ 是 $[0,\ 1]$ 上的连续函数全体, 则 $C[0,1]$ 在函数的加法和乘法下是环.

2　环的性质

性质 2.1.1　设 R 是环, 则

(1) 单位元一定是唯一的.

(2) $0 \cdot a=a \cdot 0=0$ 对任何 $a \in R$ 成立.

(3) $(-a) \cdot b=a \cdot (-b)=-(a \cdot b)$ 对任何 $a, b \in R$ 成立.

(4) $(a_1+\cdots+a_m)(b_1+\cdots+b_n)=\sum\limits_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n} a_i b_j$ 对任何 $a_1, \cdots, a_m, b_1, \cdots, b_n \in R$ 成立.

(5) 如果 $ab=ba$, 则 $(a+b)^n=\sum\limits_{i=0}^{n} C_n^i a^i b^{n-i}$.

设 $a \in R$, n 是自然数. n 个 a 相加记成 na, n 个 a 相乘记成 a^n, $(-n)a$ 可以理解为 n 个 $-a$ 相加, 也可以理解为 $-(na)$.

容易验证下面性质成立.

性质 2.1.2　设 R 是环, 则

(1) $(m+n)a=ma+na$ 对任意整数 m, n 成立;

(2) $n(a+b)=na+nb$ 对任意整数 n 成立;

(3) $m(na)=(mn)a$ 对任意整数 m, n 成立.

3 零因子和整环

若 R 是环, 则对任意 $a\in R, a\neq 0$, 都有 $0a=0, a0=0$. 在算术运算中, 容易知道, 对任意整数 a 和 b, 当 $a\neq 0, b\neq 0$ 时, 一定会有 $ab\neq 0$. 但一般情况下, 需要考虑 $a\neq 0, b\neq 0$ 时, 是否可能会有 $ab=0$ 的问题.

定义 2.1.3 *设 R 是一个环, $a\in R, a\neq 0$, 若存在 $b\in R, b\neq 0$, 满足 $ab=0(ba=0)$, 则 a 称为 b 的一个左零因子* (left zero-divisor)(*右零因子* (right zero-divisor)).

对于 $a\in R$, $a\neq 0$, 若存在 $b\in R, b\neq 0$, 满足 $ab=0$, 则 a 是 b 的一个左零因子, 容易知道, 此时 b 也是 a 的右零因子. 若 a 是 b 的一个左零因子, 也是 b 的一个右零因子, 则称 a 是 b 的一个零因子.

若环 R 零因子不存在左 (右) 零因子, 则环中的乘法消去律一定成立, 即 $a\neq 0, ab=ac(ba=ca)$ 时, 一定有 $b=c$.

定义 2.1.4 *若 R 中元素 a, b 满足 $ab=1$, 则 a 称为 b 的一个左逆元, b 称为 a 的一个右逆元. 若 $ab=ba=1$, 则 a 称为 b 的乘法逆元, 由对称性可知, 此时 b 也是 a 的乘法逆元.*

在实数域上的所有 2×2 矩阵 $M_2(\mathbf{R})$ 中, 非零元的乘积可以等于零, 如

$$a=\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix},\quad b=\begin{bmatrix}0 & 0\\ 1 & 1\end{bmatrix},$$

则 $ab=0$.

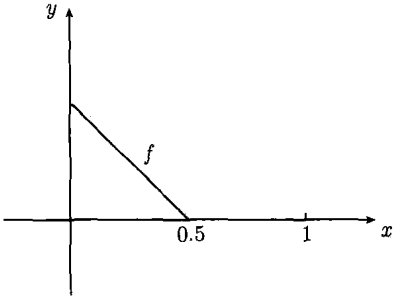
由于任意两个非零整数的乘积都不是零, 并且没有零因子的环与整数环 $\mathbf{Z}$ 有许多共同的性质, 故这类环称为整环.

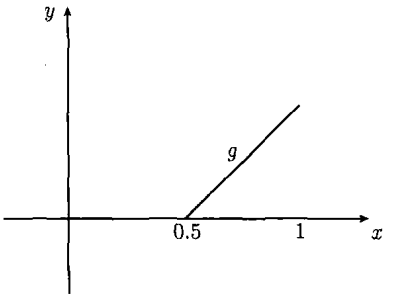
定义 2.1.5 *若非零环 R 中任何两个非零元的乘积都不等于零, 则称环 R 为整环* (integral domain).

例 2.1.6 设 $C[0,1]$ 为 $[0,1]$ 上的连续函数全体, 则环 $C[0,1]$ 不是整环. 实际上, 只需定义

$$f(x)=\begin{cases}0.5-x, & \text{当 } 0\leqslant x\leqslant 0.5 \text{ 时},\\ 0, & \text{当 } 0.5<x\leqslant 1 \text{ 时};\end{cases}\qquad g(x)=\begin{cases}0, & \text{当 } 0\leqslant x\leqslant 0.5 \text{ 时},\\ x-0.5, & \text{当 } 0.5<x\leqslant 1 \text{ 时}.\end{cases}$$

则 $f,g\in C[0,1]$, $f\neq 0, g\neq 0$, 但 $fg=0$, 所以环 $C[0,1]$ 不是整环.

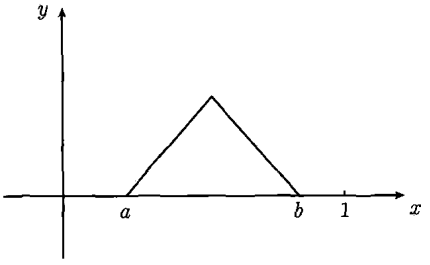




例 2.1.7　设 $C[0,1]$ 为 $[0,1]$ 上的连续函数全体构成的环, 试证明 $f\in C[0,1]$ 是零因子的充要条件为点集 $\{x\in[0,1]|f(x)=0\}$ 一定包含一个开区间.

证明　若 $f\in C[0,1]$ 是零因子, 则有 $g\in C[0,1], g\neq 0$, 使得 $fg=0$. 由 $g\neq 0$ 可知, 存在 $x\in[0,1]$, 使得 $g(x)\neq 0$. 由于 g 是连续的, 故存在开区间 $(a,b)\subseteq[0,1]$, 使得 $g(x)\neq 0$ 对任意 $x\in(a,b)$ 成立. 所以对任意 $x\in(a,b)$, 一定有 $f(x)=0$.

反过来, 若点集 $\{x\in[0,1]|f(x)=0\}$ 包含一个开区间 (a,b), 则定义



$$g(x)=\begin{cases}0, & \text{当 } 0\leqslant x\leqslant a \text{ 时},\\ x-a, & \text{当 } a<x\leqslant \dfrac{a+b}{2} \text{ 时},\\ b-x, & \text{当 } \dfrac{a+b}{2}<x\leqslant b \text{ 时},\\ 0, & \text{当 } b<x\leqslant 1 \text{ 时}.\end{cases}$$

则 $g\in C[0,1], g\neq 0$, 并且 $fg=0$, 所以 f 是零因子. ■

4　可除环

定义 2.1.6　*若非零环 R 的任何一个非零元的逆元存在, 则称 R 为一个可除环* (divisible ring).

容易知道, 可除环一定是整环.

下面的例子是 Hamilton 在 1843 年发现的, 它是数学史上第一个非交换的可除环.

例 2.1.8 设 $\mathbf{R}$ 是实数域, $H=\{a+bi+cj+dk|$ 这里 $a,b,c,d\in\mathbf{R}\}$, 定义加法

$$\begin{aligned}&(a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k)\\=&(a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k,\end{aligned}$$

则 H 是一个加法群. 如果定义

$$i^2=j^2=k^2=-1,$$

$$ij=k,\quad ki=j,\quad jk=i,$$

$$ji=-k,\quad ik=-j,\quad kj=-i,$$

则 H 是一个非交换环, 通过计算可得

$$(a+bi+cj+dk)(a-bi-cj-dk)=a^2+b^2+c^2+d^2.$$

因此 H 中每个非零元是乘法可逆的, 也就是说 H 是一个非交换的可除环, 称为**四元数可除环**(quaternion division ring), 亦称为 Hamilton **四元数可除环**.

由 $\{a+bi+cj+dk|a,b,c,d\in\mathbf{Z}\}$ 全体所构成的集合在四元数的加法和乘法下构成一个非交换环, 称为**四元整数环**.

容易知道, 若 R 是可除环, 则 $a\neq 0$ 时, 方程 $ax=b$ 都有解 $x=a^{-1}b$, 方程 $ya=b$ 都有解 $y=ba^{-1}$.

思考题 2.1.1 可除环一定是整环, 但整环一定是可除环吗?

不一定. 整数环是整环, 但它不是可除环.

5 子环

子环是环 R 的一个子集, 它是一个加法和乘法与 R 一样的环.

定义 2.1.7 设 S 是环 R 的一个非空子集, 如果在加法运算下 S 是 R 的子群, $1\in S$ 并且 $ab\in S$ 对任何 $a,b\in S$ 成立, 则称 S 为 R 的一个子环 (subring).

例 2.1.9 设 $C[0,1]$ 为 $[0,1]$ 上的连续函数全体, $C^1[0,1]$ 为 $[0,1]$ 上的连续可微函数全体, 则 $C^1[0,1]$ 是环 $C[0,1]$ 的一个子环.

容易看出, 子环可以保持环的大部分性质, 如交换环的子环仍是交换环, 整环的子环仍是整环, 但并不是所有性质都继承下来的.

思考题 2.1.2　非交换环的子环一定是非交换环吗?

不一定.

例 2.1.10　设 R 是环, R 的中心为集合 $C(R)=\{b\in R|ab=ba$ 对任意 $a\in R$ 成立 $\}$, 试证明 $C(R)$ 是 R 的交换子环.

证明　由于 $1\in C(R)$, 故 $C(R)$ 不是空集.

对任意 $a_1,a_2\in C(R)$ 和任意 $b\in R$, 有

$$a_1b=ba_1,\quad a_2b=ba_2.$$

因此

$$(a_1-a_2)b=b(a_1-a_2),$$

$$(a_1a_2)b=b(a_1a_2).$$

故

$$a_1-a_2\in C(R),\quad a_1a_2\in C(R).$$

因而, $C(R)$ 是 R 的子环. 又因为对任意 $b_1,b_2\in C(R)$, 都有 $b_1b_2=b_2b_1$, 所以 $C(R)$ 是 R 的交换子环. ■

6　子环 $R[a]$

若 R 是环 F 的子环, 则对于 $a\in F, a\notin R$, 用 $R[a]$ 记包含 R 和 $\{a\}$ 的最小的 F 的子环. 如 $\mathbf{Z}$ 为整数环, 它是实数环 $\mathbf{R}$ 的子环, $\mathbf{Z}[\sqrt{2}]$ 是包含整数环 $\mathbf{Z}$ 和 $\sqrt{2}$ 的最小的子环, 容易验证 $\mathbf{Z}[\sqrt{2}]=\{a+b\sqrt{2}|a,b\in\mathbf{Z}\}$. 另外, $\mathbf{Z}[\sqrt[3]{2}]=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}|a,b,c\in\mathbf{Z}\}$.

元素个数有限的环称为有限环, Isbell 在 1959 证明了若交换环 R 的乘法半群是有限个元素生成的, 则 R 一定是有限环①.

Ganesan 在 1964 年还证明了只有有限个零因子的交换环一定是有限环②.

① Isbell J R. On the multiplicative semigroup of commutative ring. Proc. Amer. Math. Soc., 1959, 10: 908–909.

② Ganesan N. Properties of rings with a finite number of zero divisors. Math. Ann., 1964, 157: 215–218.

2.2 理想和商环

理想是 Dedekind 1876 在他的书《数论讲义》(*Vorlesungen über Zahlentheorie*) 中首先引入的, 它是 Kummer 的理想数的推广. 理想的概念后来还得到了 Hilbert 和 Noether 的扩展和进一步研究.

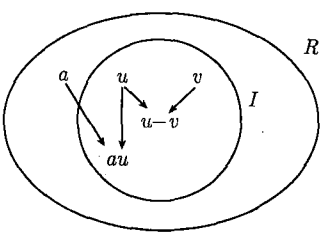
1 理想的定义

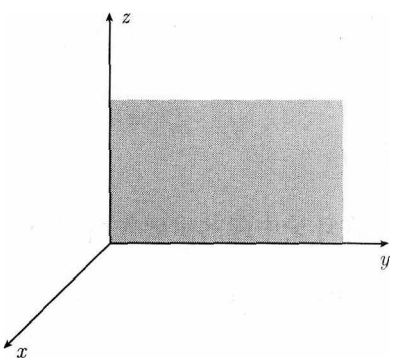
定义 2.2.1 设 I 是 R 的一个子集, 如果在加法下 I 是 R 的子群, 并且 $au \in I$ 对任何 $a \in R, u \in I$ 成立, 则 I 称为 R 的左理想.

若 $ua \in I$ 对任何 $a \in R, u \in I$ 成立, 则 I 称为 R 的右理想.

若 $au \in I$, $ua \in I$ 对任何 $a \in R, u \in I$ 都成立, 则 I 称为 R 的理想 (ideal).

例 2.2.1 在 $\mathbf{R}^3$ 按坐标的加法所构成的加法群中, 定义 $(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_1x_2, y_1y_2, z_1z_2)$, 则 $\mathbf{R}^3$ 是一个交换环, 容易看出 $\{0\}$, $\mathbf{R}^3$, X 轴, Y 轴, OYZ 平面等都是环 $\mathbf{R}^3$ 的一个理想.





反过来, 若 I 是 $\mathbf{R}^3$ 的真理想, 则存在某个 i, 使得任意 $x = (x_1, x_2, x_3) \in I$, 都有 $x_i = 0$. 实际上, 假如对任意的 $i = 1, 2, 3$ 都存在 $a, b, c \in I$, 使得 $a_1 \neq 0, b_2 \neq 0, c_3 \neq 0$, 由于 I 是 $\mathbf{R}^3$ 的理想, 故对于 $d_1 = (1, 0, 0) \in \mathbf{R}^3$, $d_2 = (0, 1, 0) \in \mathbf{R}^3$, $d_3 = (0, 0, 1) \in \mathbf{R}^3$, 有 $u = d_1a + d_2b + d_3c \in I$. 由 u 的三个分量 a_1, b_2, c_3 都不为零可知, 有 $v = \left(\dfrac{1}{a_1}, \dfrac{1}{b_2}, \dfrac{1}{c_3}\right) \in \mathbf{R}^3$, 使得 $1 = vu \in I$, 从而 $I = \mathbf{R}^3$, 与 I 是 $\mathbf{R}^3$ 的真

理想矛盾, 因而 I 是 $\mathbf{R}^3$ 的真理想时, I 中所有元的某个分量一定是 0, 所以 $\mathbf{R}^3$ 的真理想只能是 X 轴, Y 轴, Z 轴, OYZ 平面, OXZ 平面和 OXY 平面.

例 2.2.2　整数环 $\mathbf{Z}$ 中全体偶数 $2\mathbf{Z}$ 是 $\mathbf{Z}$ 的理想.

2　理想与子环的关系

思考题 2.2.1　*环 R 的理想 I 一定是 R 的子环吗?*

不一定. 如果 R 的非零理想 I 是 R 的子环, 则单位元 $1 \in I$, 因此对任意的 $a \in R$, 都有 $a = a1 \in I$, 从而 I 一定是 R. 所以环 R 的平凡理想 $\{0\}$ 和 R 都是 R 的子环, 非平凡理想都一定不是 R 的子环.

思考题 2.2.2　*环 R 的中心 $C(R) = \{b \in R | ab = ba$ 对任意 $a \in R$ 成立 $\}$ 一定是 R 的理想吗?*

不一定.

例 2.2.3　设 R 是实数域上所有的 2×2 矩阵, 则 R 的中心 $C(R)$ 为所有形如 $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ 的矩阵构成的, 但对于 $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \in R$, 有 $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} \notin C(R)$, 故 $C(R)$ 不是 R 的理想.

3　商环

理想在环论中起的重要作用, 与正规子群在群论中所起的作用是相近的.

环 R 中两个元素 a, b, 若 $a - b \in I$, 则称 a 和 b 为关于理想 I 同余, 这时记作

$$a \equiv b \,(\mathrm{mod} I)\,.$$

特别, $a \equiv 0(\mathrm{mod} I)$ 表示 $a \in I$. 容易验证, 同余是环 R 的一个等价关系, 通过这个等价关系, 可以定义商环.

定理 2.2.1　*设 I 是环 R 的一个理想, 则 R/I 在乘法 $(a+I)(b+I) = ab+I$ 下构成一个环, 称为 R 关于 I 的商环* (quotient ring).

证明　(1) 容易验算乘法运算是有意义的, 并且 R/I 在加法运算下是 Abel 群.

(2) 下面只需验证乘法的结合律和乘法对于加法的分配律. 由于

$$(a+I)[(b+I)(c+I)] = (a+I)(bc+I) = abc+I,$$

$$[(a+I)(b+I)](c+I) = (ab+I)(c+I) = abc+I,$$

故结合律成立.

由

$$\begin{aligned}(a+I)[(b+I)+(c+I)] &= (a+I)(b+c+I)\\ &= a(b+c)+I\\ &= ab+ac+I,\\ (a+I)(b+I)+(a+I)(c+I) &= (ab+I)+(ac+I)\\ &= ab+ac+I\end{aligned}$$

可知分配律成立.

类似可证

$$[(b+I)+(c+I)](a+I) = (b+I)(a+I)+(c+I)(a+I).$$

由于 $(1+I)(a+I) = 1a+I = a+I$ 对任何 $a \in R$ 成立, 所以 R/I 在乘法

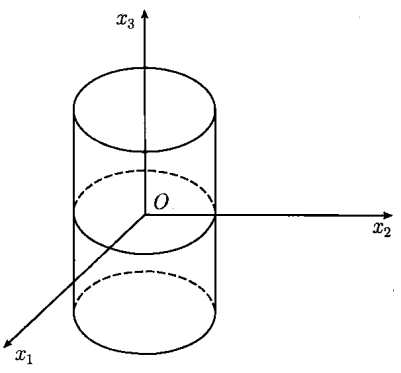
$$(a+I)(b+I) = ab+I$$

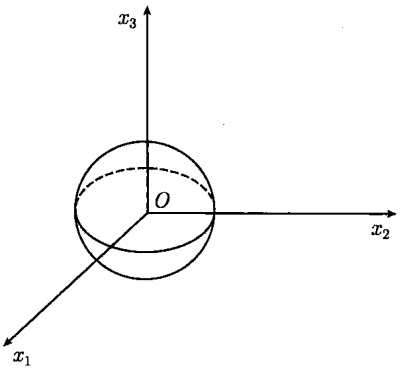
下构成一个环, $1+I$ 是 R/I 的单位元. ■

例 2.2.4 设 $\mathbf{R}$ 为实数域, $\mathbf{R}[x_1,x_2,x_3]$ 为 $\mathbf{R}$ 上的三个变量的多项式函数构成的环, 记 $M = \{(x_1,x_2,x_3) | x_1^2+x_2^2-1=0, x_3=0\}$, $I = \{f \in \mathbf{R}[x_1,x_2,x_3] |$ 对任意 $(x_1,x_2,x_3) \in M$, 都有 $f(x_1,x_2,x_3)=0\}$, 则容易验证 $f,g \in I$ 时, $f-g \in I$, 因此 I 是 $\mathbf{R}[x_1,x_2,x_3]$ 的加法子群, 并且 $f \in \mathbf{R}[x_1,x_2,x_3]$, $g \in I$ 时, 一定有 $fg \in I$. 所以 I 是多项式环 $\mathbf{R}[x_1,x_2,x_3]$ 的理想.

实际上, 容易知道, 在直角坐标系 $Ox_1x_2x_3$ 中, M 为圆柱面与 Ox_1x_2 平面的交. 由于球面 $x_1^2+x_2^2+x_3^2=1$ 也包括了 M, 故多项式 $f(x_1,x_2,x_3) = x_1^2+x_2^2+x_3^2-1$ 属于 I.

要研究直角坐标系 $Ox_1x_2x_3$ 中 M 的性质, 可以通过研究多项式环 $\mathbf{R}[x_1,x_2,x_3]$ 的理想 I 的性质来得到.





4　单环

定义 2.2.2　任何一个含多于 1 个元素的环 R 都有两个理想 0 和 R, 称为 R 的平凡理想. 如果一个环除了平凡理想外没有其他理想, 那么该环称为单环 (simple ring).

定理 2.2.2　可除环 R 一定是单环.

证明　设 I 是可除环 R 的一个理想, 若 I 不是 0 理想, 则存在非零元 $a \in I$. 由于 R 是可除环, 故 $a^{-1} \in R$, 从而 $1 = aa^{-1} \in I$. 所以对任意的 $r \in R$, 都有 $r = r1 \in I$, 因此 $R = I$, 所以 R 是单环. ■

5　理想的性质

性质 2.2.1　(1) 设 I, J 是 R 的理想, 则 $I \cap J$ 也是 R 的理想.

(2) 设 I, J 是 R 的理想, 令 $I + J = \{a + b | a \in I, b \in J\}$, 则 $I + J$ 仍是 R 的理想.

例 2.2.5　在整数环 $\mathbf{Z}$ 中, 令 $I = n\mathbf{Z}$, $J = m\mathbf{Z}$, 则

$$I \cap J = [m, n]\mathbf{Z},$$

$$I + J = (m, n)\mathbf{Z},$$

这里 $[m, n]$ 为 m 和 n 的最小公倍数, (m, n) 为 m 和 n 的最大公因子.

思考题 2.2.3　若 I, J 是环 R 中两个理想, 类似于群的乘法, 规定 I, J 的乘积为 $IJ = \{ab | a \in I, b \in J\}$, 则 IJ 一定是 R 的理想吗?

不一定. 由于 $\left\{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J, n \text{ 为某个正整数}\right\}$ 是 R 的理想, 故将它规定为理想 I 和理想 J 的乘积, 不过按照代数学历史上的习惯, 还是将它记为 IJ, 称为理想 I 和理想 J 的乘积, 但一定要注意该符号所代表的是理想乘积.

定义 2.2.3 *设 I, J 是环 R 中两个理想, 若 $I+J=R$, 则称 I, J 是互素的* (coprime).

例 2.2.6 在整数环 $\mathbf{Z}$ 中, 若 p, q 为不同的素数, 令 $I=p\mathbf{Z}$, $J=q\mathbf{Z}$, 则 I, J 是环整数环 $\mathbf{Z}$ 的两个理想, 由于 p, q 为不同的素数, 故存在 $\mathbf{Z}$ 中的 m, n, 使得 $1=mp+nq$, 从而对任意的 $r \in \mathbf{Z}$, 有 $r=rmq+rnq \in \mathbf{Z}$, 故 $I+J=\mathbf{Z}$, 所以 I, J 是互素的.

性质 2.2.2 *设 R 是环, I, J, K 都是环 R 的理想, 若 I, J 都与 K 互素的, 则 $IJ=\left\{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J, n \text{ 为某个正整数}\right\}$ 是环 R 的理想, 并且 IJ 与 K 互素.*

证明 由于 $I+K=R$, $J+K=R$, 故存在 $a \in I, k_1 \in K, b \in J, k_2 \in K$, 使得

$$a+k_1=1, \quad b+k_2=1,$$

因此

$$(a+k_1)(b+k_2)=ab+(ak_2+k_1b+k_1k_2)=1.$$

由 K 是环 R 的理想可知, $ak_2+k_1b+k_1k_2 \in K$, 因而

$$1=ab+(ak_2+k_1b+k_1k_2) \in IJ+K.$$

从而由 IJ 的定义可知, IJ 为环 R 的理想, 故 $IJ+K$ 是环 R 的理想, 因此 $IJ+K=R$, 所以 IJ 与 K 互素. ■

性质 2.2.3 *设 R 是交换环, I, J 都是环 R 的理想,*

$$IJ=\left\{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J, n \text{ 为某个正整数}\right\},$$

若 I, J 互素, 则

$$IJ=I \cap J.$$

证明 由于 I, J 都是环 R 的理想, 故明显地 $IJ \subseteq I \cap J$.

反过来, 由于 I, J 互素, 故存在 $a \in I, b \in J$, 使得 $a+b=1$, 因此对任意的 $c \in I \cap J$, 有

$$ca + cb = c.$$

由于 R 是交换环, 故 $c = ac + cb \in IJ$, 于是 $I \cap J \subseteq IJ$, 所以 $IJ = I \cap J$. ■

6　主理想

定义 2.2.4　设 R 是一个环, S 是 R 的一个非空子集, 令 (S) 为 R 中所有包含 S 的理想的交, 则 (S) 是一个理想, 称为 S 在 R 中生成的理想.

不难证明, 下面命题成立.

命题 2.2.1　设 R 是环, S 是 R 的一个非空子集, 则

$$(S) = \{a_1u_1b_1 + \cdots + a_nu_nb_n | a_1, \cdots, a_n, b_1, \cdots, b_n \in R, u_1, \cdots u_n \in S\}.$$

当 R 是交换环时, 则

$$(S) = \{a_1u_1 + \cdots + a_nu_n | a_1, \cdots, a_n \in R, u_1, \cdots, u_n \in S\}.$$

命题 2.2.2　设 R 是环, $a \in R$, 则

$$(a) = \left\{ \sum_{i=1}^{n} x_i a y_i | x_i, y_i \ \in R, n \in \mathbf{N} \right\}.$$

当 R 是交换环时, 则

$$(a) = \{ar | r \in R\}.$$

例 2.2.7　整数环 $\mathbf{Z}$ 是交换环, 对任意的整数 n, n 生成的理想 $(n) = \{kn | k \in \mathbf{Z}\}$.

例 2.2.8　$[0,1]$ 上的整数多项式函数全体是一个交换环 $P[0,1]$, 对于 $x \in P[0,1]$, 由 x 生成的理想为 $[0,1]$ 上的常数项为零的整数多项式函数全体.

定义 2.2.5　设 I 是 R 的一个理想, 如果存在 R 的一个有限子集 S 使 $I = (S)$, 则称 I 是一个有限生成的理想 (finitely generated ideal).

定义 2.2.6　若 I 可由一个元素生成, 则 I 称为一个主理想 (principal ideal).

例 2.2.9　整数环 $\mathbf{Z}$ 的每个理想都是主理想. 实际上, 若 I 是 $\mathbf{Z}$ 的一个理想, 则 I 有非零元, 故存在绝对值最小的整数 $b \in I$. 对任意的 $a \in I$, 一定有绝对值小

于 b 的 r, 使得 $a=bc+r$, 由 I 是 $\mathbf{Z}$ 的理想可知 $bc\in I$, 理想是加法子群, 故 $r\in I$, 由于 b 是 I 中绝对值最小的整数, 因而 $r=0$, 所以 $I=(b)$ 是主理想.

在交换环 R 中, 若 I 是 R 的理想, 则下面的 $\mathrm{rad}I$ 称为 I 的根.

例 2.2.10 设 I 是交换环 R 的理想, 定义

$$\mathrm{rad}I=\{r\in R|r^n\in I \text{ 对某个正整数 } n\}.$$

试证明 $\mathrm{rad}I$ 是 R 的理想.

证明 若 $r_1,r_2\in \mathrm{rad}I$, 则存在正整数 n_1,n_2, 使得 $r_1^{n_1},r_2^{n_2}\in I$, 因此 $(r_1-r_2)^{n_1n_2}\in I$, 从而 $r_1-r_2\in \mathrm{rad}I$, 故 $\mathrm{rad}I$ 是 R 的加法子群. 明显地, 对任意的 $a\in R$, $r\in \mathrm{rad}I$, 有 $r^n\in I$ 对某个正整数 n 成立, 故由 R 是交换环可知 $(ar)^n=a^nr^n\in I$, 从而 $ar\in \mathrm{rad}I$, 所以 $\mathrm{rad}I$ 是 R 的理想. ■

例 2.2.11 设 $C[0,1]$ 为 $[0,1]$ 上的连续函数全体构成的环, 试证明对于 $C[0,1]$ 的任一非平凡理想 I, 一定有实数 $x\in(0,1)$, 使得 $f(x)=0$ 对所有的 $f\in I$ 都成立.

证明 反证法, 假设对区间中每一 $x\in(0,1)$, 都存在 $f_x\in I$, 使得 $f_x(x)\neq 0$, 由于 I 是 R 的非平凡理想, 故不妨假设 $f_x(x)>0$. 由 f_x 的连续性可知, 有含 x 的某个开集 $(a_x,b_x)\subseteq(0,1)$ 使得 $f_x(y)>0$ 对任意 $y\in(a_x,b_x)$ 都成立. 再由有限覆盖定理可选出有限个这样的区间 $(a_{x_i},b_{x_i})(i=1,2,\cdots,n)$, 它们覆盖了 $[0,1]$. 从而存在 n 个连续函数 $g_{x_i}\in C[0,1]$, 使得 $h(x)=\sum\limits_{i=1}^{n}g_{x_i}(x)f_{x_i}(x)$ 为等于 1 的常值函数. 由 I 是 R 的理想可知, $h(x)\in I$, 因此 I 是 R 的含有单位元的理想, 从而 $I=C[0,1]$, 但这与 I 是 R 的非平凡理想矛盾. 所以, 一定有实数 $x\in(0,1)$, 使得 $f(x)=0$ 对所有的 $f\in I$ 都成立. ■

2.3 环的同态

环的同态是研究环的一个重要工具.

1 环同态的定义和性质

定义 2.3.1 设 R_1,R_2 是两个环, 映射 $f:R_1\to R_2$ 称为一个同态 (homomorphism), 如果

(1) 对任何 $a,b\in R_1$, 都有 $f(a+b)=f(a)+f(b)$;

(2) 对任何 $a,b\in R_1$, 都有 $f(ab)=f(a)f(b)$;

(3) $f(1)=1$.

性质 2.3.1　设 R_1,R_2 是环, $f:R_1\to R_2$ 为同态, 则

(1) 同态 $f:R_1\to R_2$ 把 R_1 的零元映成 R_2 的零元;

(2) 对任意 $a\in R_1$ 和正整数 n, 有 $f(a^n)=f(a)^n$;

(3) 对任意乘法可逆元 $a\in R_1$, 有 $f(a^{-1})=f(a)^{-1}$.

例 2.3.1　设 $\mathbf{Z}$ 为整数环, $\mathbf{R}$ 为实数环, $f:\mathbf{Z}\to\mathbf{R}, a\mapsto a$, 则 f 为 $\mathbf{Z}$ 到 $\mathbf{R}$ 的同态.

定义 2.3.2　设 R_1,R_2 是环, $f:R_1\to R_2$ 为同态, 称 $\mathrm{Ker}(f)=\{a\in R_1|f(a)=0\}$ 为 f 的核 (kernel). 称 $\mathrm{Im}(f)=\{f(a)|a\in R_1\}$ 为 f 的像 (image).

明显地, 有如下性质成立.

性质 2.3.2　f 是单射当且仅当 $\mathrm{Ker}(f)=\{0\}$.

定义 2.3.3　f 是单射时, 称 f 为一个单同态 (monomorphism). f 是满射时, 称 f 为一个满同态 (epimorphism). 如果一个同态 f 既是单同态又是满同态, 即 f 是双射, 则 f 称为一个同构 (isomorphism). 如果在两个环 R_1,R_2 之间存在一个同构, 则称这两个环是同构的, 记作 $R_1\cong R_2$. 从环 R 到 R 的一个同构称为自同构 (automorphism).

例 2.3.2　设 C 是复数域, $f:C\to C$, 对任意 $a+b\mathrm{i}\in C$, 定义 $f(a+b\mathrm{i})=a-b\mathrm{i}$, 则 f 为 C 到 C 的同构.

例 2.3.3　设 R_1,R_2 是环, $f:R_1\to R_2$ 为同态, $u,v\in\mathrm{Ker}(f), a\in R_1$, 试证明 $u+av\in\mathrm{Ker}(f)$.

证明　由于 $f(u)=0, f(v)=0$, 故 $f(u+av)=f(u)+f(a)f(v)=0$, 所以 $u+av\in\mathrm{Ker}(f)$. ■

2　环的同态和同构定理

定理 2.3.1(环同态基本定理)　设 $f:R_1\to R_2$ 是一个环同态, 则 $\mathrm{Ker}(f)$ 是

R_1 的真理想, 且

$$R_1/\mathrm{Ker}(f) \cong \mathrm{Im}(f).$$

证明 设 $a \in R_1, h \in \mathrm{Ker}(f)$, 则

$$f(ah) = f(a)f(h) = f(a)0 = 0,$$

$$f(ha) = f(h)f(a) = 0f(a) = 0,$$

故 $ah \in \mathrm{Ker}(f), ha \in \mathrm{Ker}(f)$, 因而 $\mathrm{Ker}(f)$ 是 R_1 的理想. 由于 $f(1) = 1$, 故 $1 \notin \mathrm{Ker}(f)$, 所以 $\mathrm{Ker}(f)$ 是 R_1 的真理想.

记 $I = \mathrm{Ker}(f)$, 根据群的同态基本定理, 存在群同构:

$$\varphi : R_1/I \to \mathrm{Im}(f), \quad a + I \to f(a).$$

因为 $\varphi((a+I)(b+I)) = \varphi(ab+I) = f(ab) = f(a)f(b) = \varphi(a+I)\varphi(b+I)$, 所以 $R_1/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. ■

由上面环的定理可知, 研究环的同态像的性质, 等价于研究相应环的商环的性质. 类似群的第一同构定理和第二同构定理, 环也有第一同构定理和第二同构定理.

定理 2.3.2(环第一同构定理) 设 S 是环 R 的一个子环, I 是 R 的一个理想, 则 $S+I = \{a+b|a \in S, b \in I\}$ 是 R 的子环, I 是 $S+I$ 的理想, $S \cap I$ 是 S 的理想, 且

$$(S+I)/I \cong S/(S \cap I).$$

证明 明显地, $S+I$ 是 R 的加法子群. 设 $a_1, a_2 \in S, b_1, b_2 \in I$, 则

$$(a_1+b_1)(a_2+b_2) = a_1a_2 + (a_1b_2 + b_1a_2 + b_1b_2) \in S+I.$$

因此 $S+I$ 是 R 的子环.

容易验证 I 是 $S+I$ 的理想, $S \cap I$ 是 S 的理想.

作映射 $f : S \to (S+I)/I, a \to a+I$. 则 f 是一个满同态. 而且 $\mathrm{Ker}(f) = S \cap I$, 从而根据同态基本定理, 有 $(S+I)/I \cong S/(S \cap I)$. ■

不难验证下面定理成立.

定理 2.3.3(环第二同构定理) 设 R 是一个环, I, J 都是 R 的理想, 并且 $I \subseteq J$, 则 J/I 是 R/I 的理想, 并且

$$(R/I)/(J/I) \cong R/J.$$

命题 2.3.1　*若集合 S 满足环定义中的条件 (1), (2) 和 (3), 但 S 没有单位元, 则存在有单位元的环 R 和 $f: S \to R$, 满足*

$$f(a+b) = f(a) + f(b), f(ab) = f(a)f(b),$$

并且 f 是单射.

证明　令 $H = \{(a,m) | a \in R, m \in Z\}$, 对任意的 $(a,m) \in H, (b,n) \in H$, 定义

$$(a,m) + (b,n) = (a+b, m+n),$$

$$(a,m)(b,n) = (ab + na + mb, mn),$$

则不难验证, H 关于上面的定义构成一个环.

对任意的 $(a,m) \in H$, 有

$$(a,m)(0,1) = (a0 + 1a + m0, m1) = (a,m),$$

$$(0,1)(a,m) = (0a + m0 + 1a, 1m) = (a,m),$$

故 $(0,1)$ 是 R 的单位元.

对任意的 $a, b \in S$, 定义 $f: S \to R, a \mapsto (a,0)$, 则容易验证

$$f(a+b) = f(a) + f(b), f(ab) = f(a)f(b),$$

并且 f 是单射. ■

由上面命题可知, 若 S 满足环定义中的条件 (1), (2) 和 (3), 但 S 没有单位元, 则 S 可嵌入含有单位元的环 R 中.

例 2.3.4　设 $\mathbf{R}[x]$ 为实数多项式全体所构成的环, 对于

$$f(x) \in \mathbf{R}[x], f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

令 $\varphi: \mathbf{R}[x] \to \mathbf{R}$, $f(x) \mapsto a_0$, 则 φ 是 $\mathbf{R}[x]$ 到实数域 $\mathbf{R}$ 的满同态, 不难验证 $\mathrm{Ker}(\varphi)$ 是 x 生成的理想, $\mathrm{Ker}(\varphi) = \{a_n x^n + \cdots + a_1 x | a_i \in \mathbf{R}\}$, 并且 $\mathbf{R}[x]/\mathrm{Ker}(\varphi) \cong R$.

Herstein 在 1961 年得到了下面很有意思的结果①.

定理 2.3.4　*设 R 是环, 若对于某个固定的 $n > 1$, R 到 R 的映射 $f: a \to a^n$ 是环同态, 并且它是满的, 则 R 一定是交换环.*

① Herstein I N. Power maps in rings. Michigan Math. J., 1961, 8: 29–32.

2.4 域

全体有理数组成的整环 $\mathbf{Q}$ 和全体实数组成的整环 $\mathbf{R}$, 都具有整数环 $\mathbf{Z}$ 所不具备的重要的代数特征: 在 $\mathbf{Q}$ 和 $\mathbf{R}$ 中, 任何方程 $ax=b$ 都是可解的, 具有该性质的交换环称为域. 伽罗瓦关于代数方程的著作中就有了域的概念的萌芽, Dedekind 和 Kronecker 也提出了域的概念, 对域的系统研究最早是 Weber, 他在 1893 年的论文 *Die allgemeinen grundlagen der Galois'schen gleichungstheorie* 给出了域的抽象定义. Dickson 和 Huntington 分别于 1903 年和 1905 年独立地创立了域的公理系统.

Strinitz 系统地研究了抽象的域, 并在 1901 发表了 "域的代数理论".

1 域的定义

定义 2.4.1 一个交换可除环称为域 (field). 域的子环如果是域, 则称为一个子域 (subfield).

例 2.4.1 由于有理数环 $\mathbf{Q}$, 有理数环是可除环, 它还是交换的, 故它是一个域. 全体整数在加法和乘法下构成一个整环, 但它不是域.

Heinrich Weber(1842—1913)

例 2.4.2 设 p 是一个素数, 试证明剩余类环 $\mathbf{Z}_p$ 是一个域.

证明 不难验证 $\mathbf{Z}_p=\{\overline{0},\overline{1},\cdots,\overline{p-1}\}$ 是一个有单位元的交换环.

对于 $\mathbf{Z}_p$ 的任意一个非零元 $\overline{a}$, 不妨设 $1<a\leqslant p-1$, 由于 p 是素数, 故 $(a,p)=1$, 从而存在 u,v, 使得

$$ua+vp=1.$$

因此 $\overline{ua}+\overline{vp}=\overline{ua+vp}=\overline{1}$, 又因为 $\overline{vp}=0$, 所以 $\overline{u}\,\overline{a}=\overline{ua}=\overline{1}$, 即 $\overline{a}$ 是可逆元, 所以剩余类环 $\mathbf{Z}_p$ 是一个域. ■

特别的, 当 p 为 2 时, $\mathbf{Z}_2$ 只有两个元素, 它的加法表和乘法表都很简单.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$	$\overline{1}$

实际上, Gauss 早在 1801 年在他的算术专论中就研究了素数域 $\mathbf{Z}_p$, 并且证明了 $\mathbf{Z}_p$ 有循环的乘法群.

2　域中的理想

由于域本身是环, 故可以讨论域中的理想.

性质 2.4.1　*设 I 是域 F 的理想, 则 I 是 $\{0\}$ 或 F.*

证明　若 I 是域 F 的理想, I 不是理想 $\{0\}$, 则存在 $a \in I, a \neq 0$. 由于 F 是域, 故存在 $a^{-1} \in F$, 因而 $1 = aa^{-1} \in I$, 所以 I 等于 F. ■

由此知道, 域中的理想没有太多的意义, 要像环一样用理想来研究域的性质是行不通的, 域的研究需要新的方法.

3　域的同态

两个域或域与环之间的同态是指将域看做环时的同态, 它们都比较简单.

性质 2.4.2　*设 $f : F \to A$ 是从一个域到一个环的同态, 若 $A \neq 0$, 则 f 一定是单同态.*

证明　由于 $A \neq 0$, 故 $f(1_F) = 1_A \neq 0$, 因此 $\mathrm{Ker}(f)$ 是 F 的一个真理想, 它只能是 0. 所以, f 是单同态. ■

4　分式域

从整数出发, 容易构造出有理数, 因此可以模仿从整数到分数的方式从一个给定的交换整环 R 来构造域.

定义 2.4.2　*设 R 是交换整环, 令 $F = \left\{\dfrac{b}{a} | a, b \in R, a \neq 0\right\}$, 规定等价关系 $a_1/b_1 \approx a_2/b_2$ 当且仅当 $a_1 b_2 = a_2 b_1$.*

F 的加法和乘法运算为

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2},$$

$$\frac{a_1}{b_1}\frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}.$$

容易验证加法和乘法都是合理的, 并且在加法下 F 是 Abel 群, 其零元是 $\frac{0}{1}$. 乘法满足结合律、交换律和对加法的分配律, $\frac{1}{1}$ 是单位元, 每个非零元 $\frac{a}{b}$ 有可逆元 $\frac{b}{a}$, 因此 F 是一个域, 称为 R 的分式域 (field of fractions).

令 $J: R \to F, a \mapsto \frac{a}{1}$. 则 J 是一个单同态, 因此 R 可以看成它的分式域的一个子环.

例 2.4.3 有理数域 $\mathbf{Q}$ 是整数环 $\mathbf{Z}$ 的分式域.

5 极大理想

定义 2.4.3 设 I 是环 R 的一个理想, $I \neq R$, 若 I 和 R 之间没有其他理想, 则称 I 是 R 的一个极大理想 (maximal ideal).

例 2.4.4 设 p 是素数, 则主理想 (p) 是整数环 $\mathbf{Z}$ 的极大理想. 实际上, 若 I 为 $\mathbf{Z}$ 的理想, 并且 $(p) \subseteq I \subseteq \mathbf{Z}$, $(p) \neq I$, 则存在 $m \in I$, 但 $m \notin (p)$, 因此 m 和 p 互素, 故存在 u 和 v, 使得 $um + vp = 1$, 因而由 $um \in I, vp \in (p) \subseteq I$ 可得 $1 \in I$, 所以 $I = \mathbf{Z}$.

例 2.4.5 设 F 是实数域, $F[x]$ 为 F 上的多项式环, 则主理想 (x) 是 $F[x]$ 的极大理想. 实际上, 若 I 为 $F[x]$ 的理想, 并且 $(x) \subseteq I \subseteq F[x]$, $(x) \neq I$, 则存在 $f(x) \in I$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, 并且 $a_0 \neq 0$. 令

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x,$$

则容易知道 $g(x) \in (x) \subseteq I$, 从而 $a_0 = f(x) - g(x) \in I$, 因此, $1 \in I$, 所以 $I = F[x]$.

例 2.4.6 设 $C[0,1]$ 为 $[0,1]$ 上的连续函数全体构成的环, 试证明 $I = \{f \in C[0,1] | f(0) = 0\}$ 是 $C[0,1]$ 的极大理想.

证明 设 J 是 $C[0,1]$ 的一个包含 I 的理想并且 $J \neq I$, 则存在 $f \in J, f \notin I$, 故 $f(0) \neq 0$. 令 $g(x) = 1 - \frac{f(x)}{f(0)}$, 则 $g(0) = 0$, 因此 $g \in I \subseteq J$, 由 J 是理想可知 $\frac{1}{f(0)} f(x) \in J$, 因而 $1 = g(x) + \frac{1}{f(0)} f(x) \in J$, 故 $J = C[0,1]$, 所以 J 是 $C[0,1]$ 的极大理想. ■

命题 2.4.1 设 I 是交换环 R 的一个理想, 则 R/I 是一个域当且仅当 I 是 R 的一个极大理想.

证明　设 R/I 是域, 欲证 I 是 R 的一个极大理想. 若 J 是 R 的一个包含 I 的理想并且 $J \neq I$. 任取 $a \in J, a \notin I$, 则 $a+I$ 是 R/I 中的非零元, 因此存在 $b+I$, 使得 $(a+I)(b+I) = 1+I$, 从而 $ab-1 \in I$. 记 $u = ab-1$, 则 $u \in I$, $1 = ab-u$. 由于 $a \in J$, J 是 R 的理想, 故 $ab \in J$, 从而由 $u \in I \subseteq J$ 可知 $ab-u \in J$, 故 $1 \in J$, 因此 $J = R$, 所以 I 是 R 的一个极大理想.

反过来, 设 I 是 R 的一个极大理想. 设 $a \in R, a \notin I$, 令 J 为由 I 和 a 生成的理想. 根据极大理想定义得 $J = R$, 故 $1 \in J$, 由于 $J = (I \cup \{a\}) = \{ba+u | u \in I, b \in R\}$, 故存在 $a \in R, u \in I$, 使得 $1 = ba+u$, 由于 $ab = 1-u$, 故 $(a+I)(b+I) = 1+I$, 因此 $a+I$ 是可逆元, 所以 R/I 是一个域. ■

思考题 2.4.1　*设 R 是一个环, 则 R 的极大理想是否一定唯一?*

不一定, 如整数环 $\mathbf{Z}$, $\mathbf{Z}$ 有极大理想 (2), (3) 和 (7) 等.

6　整环和域的特征

定义 2.4.4　*设 R 是一个整环, a 是 R 的非零元, 若存在某个正整数 m, 使得 $ma = 0$, 就称 a 是周期元. 若 m 是使得 $ma = 0$ 的最小非负整数, 则称 m 为 a 的周期.*

定理 2.4.1　*设 R 是一个整环, 若 R 至少含有一个周期元, 则一定存在素数 p, 使得对 R 的一切非零元 a, 都有 $pa = 0$, 这个 p 就称为环 R 的特征* (characteristic).

证明　若 a 是 R 的非零元, $ma = 0$, 则对任意的 $b \in R$, 有 $(ma)b = 0$, 故 $a(mb) = 0$. 由于 R 是一个整环, 故 $mb = 0$. 记使得 $ma = 0$ 的最小正整数为 p, 如果 p 不是素数, 则存在 m_1, m_2, 使得 $p = m_1 m_2$. 由 $m_1 m_2 a = pa = 0$ 可知, $m_1 m_2 a = m_1 m_2 (1a) = (m_2 1)(m_1 a) = 0$, 故 $m_1 a = 0$ 或 $m_2 a = 0$, 但这与 p 是最小正整数矛盾, 所以一定存在素数 p, 使得对 R 的一切非零元 a, 都有 $pa = 0$. ■

若 R 不是整环, 是否可以定义特征呢?

思考题 2.4.2　*设 R 是环, 是否存在素数 p, 使得对 R 的一切非零元 a, 都有 $pa = 0$ 吗?*

不一定. 实际上, 在环 $\mathbf{Z}_2 \oplus \mathbf{Z}_3$ 中, $(1,0)$ 的周期为 2, 但 $(0,1)$ 的周期是 3, 因此在 $\mathbf{Z}_2 \oplus \mathbf{Z}_3$ 不存在素数 p, 使得对 $\mathbf{Z}_2 \oplus \mathbf{Z}_3$ 的一切非零元 a, 都有 $pa = 0$.

定义 2.4.5　*设 R 是一个整环, R 没有周期元, 则称该环的特征为零.*

容易知道, 由于域也是整环, 故环的特征概念在域中, 也是适用的.

定理 2.4.2 任何一个特征为零的域 F 包含一个同构于有理数域 $\mathbf{Q}$ 的子域.

证明 由于域 F 的特征为零, 故对任意的非零正整数 m, 都有 $m\cdot 1\neq 0$. 定义 $f:\mathbf{Q}\to F,\ \dfrac{p}{q}\mapsto (p\cdot 1)(q\cdot 1)^{-1}$(这里 $q\neq 0$), 则不难验证 f 的定义是合理的, 并且 f 是单同态, 所以 $\mathbf{Q}$ 与 F 的子域 $f(F)$ 同构. ■

定理 2.4.3 任何一个特征为素数 $p>0$ 的域 F 包含一个最小的子域, 它同构于 $\mathbf{Z}_p$.

证明 设域 F 的特征为 p, 1 为 F 的单位元, 记由 1 生成的 F 的子域为 F_p. 明显地, $F_p=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{p-1}\}$, 这里 $\overline{k}=1+1+\cdots+1(k\text{ 个 }1)$. 由于 F 的任何子域都包含 1, 故它一定也包含 F_p, 因而 F_p 是 F 最小的子域.

定义 $\varphi:\mathbf{Z}_p\to F_p,\overline{k}\mapsto\overline{k}$, 则不难验证, φ 是域同构, 所以特征为 p 的域 F 一定与 $\mathbf{Z}_p$ 同构. ■

下面的公式是很有用的.

命题 2.4.2 设 F 是特征等于素数 $p>0$ 的域, $a,b\in F$, r 是一个自然数, 则

$$(a+b)^{p^r}=a^{p^r}+b^{p^r}.$$

证明 用归纳法对 r 进行归纳证明. 当 $r=1$ 时, 有

$$(a+b)^p=\sum_{i=0}^{p}C_p^i a^i b^{p-i}.$$

对于 $1<i<p$, 自然数 C_p^i 被 p 整除, 所以 $C_p^i a^i b^{p-i}=0$ 对所有 $0<i<p$ 成立. 因此

$$(a+b)^p=a^p+b^p.$$

因而命题对 $r=1$ 成立.

假设命题对小于等于 r 都成立, 则对 $r+1$, 有

$$\begin{aligned}(a+b)^{p^{r+1}}&=[(a+b)^{p^r}]^p\\&=(a^{p^r}+b^{p^r})^p\\&=(a^{p^r})^p+(b^{p^r})^p\\&=a^{p^{r+1}}+b^{p^{r+1}}.\end{aligned}$$

因而命题对 $r+1$ 也成立. 所以由归纳原理可知命题成立. ■

定理 2.4.4　设 F 是特征等于素数 p 的交换整环, $a \in F$, 则 $f: F \to F, a \mapsto a^p$ 是环同态.

证明　由上面命题可知 $(a \pm b)^p = a^p \pm b^p$, 故 $f(a \pm b) = f(a) \pm f(b)$. 明显地, $f(ab) = f(a)f(b) = a^p b^p$, 因此 $f(1) = f(1)f(1) = 1^p \cdot 1^p = 1$, 所以 f 是环同态. ■

推论 2.4.1　在特征为素数 p 的有限域 F 中, $a \in F$, 则 $f: F \to F, a \mapsto a^p$ 是环自同构.

证明　在有限域 F 中, 若 $a^p = 0$, 则 $a = 0$(否则由 a 可逆可得出矛盾), 因此同态 f 核是零, 从而同态 f 是单射. 由于 F 是有限的, 故 f 一定是满射, 所以 f 是一个自同构. ■

7　素理想

1871 年 Dedekind 将素数的概念推广为素理想.

定义 2.4.6　设 R 是交换环, 若 I 是 R 的理想, 并对任意的 $a, b \in R$, 当 $ab \in I$ 时, 一定有 $a \in I$ 或 $b \in I$, 则称 I 为素理想 (prime ideal).

例 2.4.7　设 p 是素数, 则主理想 (p) 是整数环 $\mathbf{Z}$ 的素理想. 实际上, 对 $a, b \in Z$, 当 $ab \in (p)$ 时, 一定有 p 整除 a 或 p 整除 b, 因此 $a \in (p)$ 或 $b \in (p)$.

命题 2.4.3　设 I 是交换环 R 的一个理想, 则 R/I 是一个整环当且仅当 I 是 R 的一个素理想.

证明　设 R/I 是整环, 对任意的 $a, b \in R$, 当 $ab \in I$ 时, 由于

$$(a+I)(b+I) = ab + I = I,$$

故 $a + I = I$ 或者 $b + I = I$, 因而 $a \in I$ 或者 $b \in I$, 所以 I 是素理想.

反过来, 设 I 是 R 的素理想. 在 R/I 中, 若 $(a+I)(b+I) = I$, 则 $ab \in I$, 故 $a \in I$ 或者 $b \in I$, 因而 $a + I = I$ 或者 $b + I = I$, 因此没有真零因子, 所以 R/I 是一个整环. ■

推论 2.4.2　交换环 R 的极大理想 I 一定是素理想.

思考题 2.4.3　交换环 R 的素理想 I 一定是极大理想吗?

不一定. 实际上, 对于整数多项式 $\mathbf{Z}[x]$, $I=(x)$ 为所有常数项为 0 的整数多项式, 有 $\mathbf{Z}[x]/I\cong Z$, 由于 $\mathbf{Z}$ 是整环, 但不是域, 故 I 是 $\mathbf{Z}[x]$ 的素理想, 但它不是 $\mathbf{Z}[x]$ 的极大理想.

8 准素理想

在整数环 $\mathbf{Z}$ 中, 理想 (8) 不是素理想, 但对任意 $ab\in(8)$, 若 $a\notin(8)$, 则 b 一定是偶数, 因此 $b^3\in(8)$.

定义 2.4.7 设 R 是交换环, 若 I 是 R 的理想, 并对任意的 $a,b\in R$, 当 $ab\in R$, $a\notin I$ 时, 一定有整数 $n>0$, 使得 $b^n\in I$, 则称 I 为准素理想 (primary ideal).

准素理想的定义是 Lasker 在 1905 年给出的. 明显地, 素理想一定是准素理想, 准素理想是素理想的推广, 因此可以考虑如下的问题.

思考题 2.4.4 交换环 R 的准素理想具有哪些性质?

可以与理想一样讨论准素理想的性质, 如准素理想的交是否一定是准素理想等.

2.5 环上的微分

在数学分析中, 如果函数 $f(x)$ 和 $g(x)$ 可微, 那么

(1) $\mathrm{d}[f(x)\pm g(x)]=\mathrm{d}f(x)\pm\mathrm{d}g(x)$;

(2) $\mathrm{d}[f(x)g(x)]=g(x)\mathrm{d}f(x)+f(x)\mathrm{d}g(x)$;

(3) $\mathrm{d}\left[\dfrac{f(x)}{g(x)}\right]=\dfrac{g(x)\mathrm{d}f(x)-f(x)\mathrm{d}g(x)}{g(x)^2}$;

(4) $\mathrm{d}[f(g(x))]=f'(u)g'(x)\mathrm{d}x$(这里 $f(u)$ 和 $g(x)$ 都可微).

1 微分的定义

类似的, 在环上也可以定义抽象的微分.

定义 2.5.1 设 R 是个环, 映射 $\partial:R\to R$, 如果对任意 $a,b\in R$, 都有

(1) $\partial(a+b)=\partial a+\partial b$;

(2) $\partial(ab) = (\partial a)b + a\partial b$.

则称 ∂ 为环 R 的一个微分.

明显地, 若在环 R 上定义 $\partial : R \to R, a \mapsto 0$, 则 ∂ 一定是 R 的一个微分.

例 2.5.1　有理数 $\mathbf{Q}$ 上的多项式环 $\mathbf{Q}[x]$ 上, 微积分中的求导运算 ∂ 就是环 $Q[x]$ 上的一个微分.

容易验证下面结论成立.

定理 2.5.1　任意环 R 上的所有微分全体构成一个环.

思考题 2.5.1　任意环 R 都存在微分吗?

实际上, 若 R 是环, d 是 R 的元素, 令

$$\partial_d a = ad - da,$$

则对任意 $a, b \in R$, 有

(1) $\partial_d(a+b) = (a+b)d - d(a+b) = (ad - da) + (bd - db) = \partial_d a + \partial_d b$;

(2) $\partial_d(ab) = (ab)d - d(ab) = (ad)b - (da)b + a(bd) - a(db) = (\partial_d a)b + a(\partial_d b)$.

因此 ∂_d 为环 R 的一个微分, 称之为由元素 d 决定的内微分.

性质 2.5.1　设 R 是环, 则对任意 $d \in C(R) = \{a \in R | ab = ba$ 对任意 $b \in R\}$, 都有 ∂_d 为零映射.

2　微分的性质

性质 2.5.2　设 R 是交换环, 则对任意 $a \in R$, 有 $\partial(a^2) = 2a\partial a$.

证明　这是由于 $\partial(a^2) = \partial(aa) = (\partial a)a + a\partial(a) = 2a\partial a$.

为了简明, 按照数学分析的习惯, 将环 R 上的微分 ∂a 记为 a', 则可将微分定义中的形式改成:

$$(a+b)' = a' + b',$$

$$(ab)' = a'b + ab'.$$

定理 2.5.2　若 R 是一个环, 则 R 的单位元的微分一定是零.

证明 由于 $1'=(1\cdot 1)'=1'\cdot 1+1\cdot 1'=1'+1'$, 故 $1'=0$. ■

定义 2.5.2 *设 R 是个环, 若 $a\in R, a'=0$, 则称 a 为常元.*

容易验证, 下面结论成立.

定理 2.5.3 *若 R 是一个环, 则 R 的常元全体 $S=\{a\in R|a'=0\}$ 是 R 的一个子环.*

例 2.5.2 试证明整数环 $\mathbf{Z}$ 上的微分都一定是零微分.

证明 对整数环 $\mathbf{Z}$ 上的微分, 都有 $1'=0$, 因此任意元 $n\in\mathbf{Z}$, 有

$$n'=(1+1+\cdots+1)'=1'+1'+\cdots+1'=0.$$

所以, 整数环 $\mathbf{Z}$ 上的微分都是零微分. ■

2.6 拓 扑 环

拓扑环是环与拓扑空间的结合, 环上的拓扑保证了环运算的连续. 拓扑环是 Dantzig 在 1931 年引入的①.

1 拓扑环

定义 2.6.1 *如果 R 是环, (R,τ) 是拓扑空间, 并且*

(1) *对任意的 $a,b\in R$, 环的运算 $(a,b)\to a+b$ 是 $R\times R\to R$ 的连续映射.*

(2) *对任意的 $a,b\in R$, 环的运算 $a\to -a$ 是 $R\to R$ 的连续映射.*

(3) *对任意的 $a,b\in R$, 环的运算 $(a,b)\to ab$ 是 $R\times R\to R$ 的连续映射.*

那么环 R 称为拓扑环.

例 2.6.1 设 $\mathbf{R}$ 为全体实数, τ 为所有开区间生成的拓扑, 则实数环 $\mathbf{R}$ 是一个拓扑环.

① van Dantzig D. Studiën over topologische algebra. Dissertation, Amsterdam, H. J. Paris, 1931.

2　赋范环

定义 2.6.2　设 R 是环, 若 $||\cdot||$ 为 $R \to [0,+\infty)$ 的映射, 并对任意 $x,y \in R$, 有

(1) $||0|| = 0$;

(2) $||x+y|| \leqslant ||x|| + ||y||$;

(3) $||-x|| = ||x||$;

(4) $||xy|| \leqslant ||x||||y||$;

(5) 若 $||x|| = 0$, 则 $x = 0$.

则称 $||\cdot||$ 为环 R 的范数, 此时 R 称为赋范环.

若 R 是赋范环, 则 $d(x,y) = ||x-y||$ 为 R 上的一个**度量**. 即 $d(x,y)$ 为 R 到 $(-\infty,+\infty)$ 的映射, 它满足:

(1) $d(x,y) = 0$ 当且仅当 $x = y$;

(2) $d(x,y) = d(y,x)$;

(3) $d(x,y) \leqslant d(x,z) + d(y,z)$.

容易知道, 环 R 上的度量就是距离的推广. 在实数域 R 上定义 $||x|| = |x|$, 则容易验证 $||\cdot||$ 为实数域 R 上的范数, $d(x,y) = ||x-y||$ 为 R 上 x 点到 y 点的距离.

定理 2.6.1　若 $||\cdot||$ 是环 R 上的范数, $d(x,y) = ||x-y||$, 则 R 在度量拓扑下是拓扑环.

证明　若 $a,b \in R$, 则对任意 $x,y \in R$, 有

$$\begin{aligned} d(x+y,a+b) &= ||(x+y)-(a+b)|| \\ &\leqslant ||x-a|| + ||y-b|| \\ &= d(x,a) + d(y,b), \end{aligned}$$

因此环 R 的加法运算对于度量拓扑是连续的.

由 $d(-x,-a) = ||-x+a|| = ||x-a|| = d(x,a)$ 可知, 环 R 的运算 $a \to -a$ 对于度量拓扑是连续的.

由于

$$\begin{aligned} d(xy, ab) &= ||xy - ab|| \\ &\leqslant ||(x-a)(y-b) + a(y-b) + b(x-a)|| \\ &\leqslant ||x-a|| \cdot ||y-b|| + ||a|| \cdot ||y-b|| + ||b|| \cdot ||x-a||, \end{aligned}$$

故环 R 的乘法运算对于度量拓扑是连续的, 所以环 R 是度量拓扑下的拓扑环. ■

例 2.6.2 设 $C'[0,1]$ 为 $[0,1]$ 上所有在 $(0,1)$ 内连续可导, 并且 $\lim\limits_{t\to 0^+} a'(t)$ 和 $\lim\limits_{t\to 1^-} a'(t)$ 都存在的函数, 则 $C'[0,1]$ 在函数的加法和乘法下是一个环, 定义

$$||a|| = \sup\{|a(t)||0 \leqslant t \leqslant 1\} + \sup\{|a'(t)||0 < t < 1\}.$$

容易验证 $C'[0,1]$ 在 $||\cdot||$ 下是一个赋范环.

例 2.6.3 设 l_1 为所有绝对收敛的实数列, 即 $l_1 = \left\{(a_i)|\sum\limits_{i=1}^{\infty}|a_i| < +\infty\right\}$, 定义 $(a_i)+(b_i) = (a_i+b_i), (a_i)(b_i) = (a_ib_i)$, 则 l_1 是一个环. 并且 $||(a_i)|| = \sum\limits_{i=1}^{\infty}|a_i|$ 是 l_1 的一个范数, 因此 l_1 在该范数下是赋范环.

Anzai 在 1943 年研究了紧拓扑环的一些性质, 并证明了若紧拓扑环 R 是连通的, 则对所有的 $x, y \in R$, 有 $xy = 0$[①]. Kaplansky 发表了一系列论文[②③], 研究了紧拓扑环和局部紧拓扑环, 得到了紧拓扑环和局部紧拓扑环的构造定理等. Arnautov; M. I. Vodinčar 在 1968 年研究了拓扑环一般的根理论[④].

3 Noether 环和 Artin 环简介

顺便指出, 环论中研究比较多的还有 Noether 环、Artin 环和 Dedekind 环等, 不过这些环的定义一般没有包含单位元的要求. 升链条件是 1921 年 Noether 在研究理想分解时提出来的.

定义 2.6.3 若环 R 的理想的任何无穷升链 $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$, 都存在正整数 n, 使得当 $i \geqslant n$ 时, 都有 $I_i = I_n$, 则称 R 为 Noether 环 (Noetherian ring).

① Anzai H. On compact topological rings. Proc. Imp. Acad. Tokyo, 1943, 19: 613–615.

② Kaplansky I. Topological rings. Amer. J. Math., 1947, 69: 153-183.

③ Kaplansky L. Locally compact rings. Amer. J. Math., 1948, 70: 447–459.

④ Arnautov V I, Vodinčar M I. Radicals of topological rings. (Russian) Mat. Issled. 1968, 3, 2(8): 31–61.

不难验证, 整数环 $\mathbf{Z}$ 是 Noether 环.

Cohen 证明了下面的结果.

定理 2.6.2　*交换环 R 是 Noether 环 (有单位元) 的充要条件为 R 的每个素理想都是有限生成的.*

定理 2.6.3　*设 R 是 Noether 环, I 是 R 的理想, R/I 也是一个 Noether 环.*

1890 年, Hilbert 证明了著名的 Hilbert 基定理.

定理 2.6.4　*若 R 是 Noether 环, 则 $R[x]$ 也是一个 Noether 环.*

Artin 在 1927 提出了用降链条件来区别环, 他把 Wedderburn 定理推广到满足降链条件的环, 得到了满足降链条件的环的构造定理, 因此满足降链条件的环就称为 Artin 环.

定义 2.6.4　*若环 R 的左 (右) 理想的任何无穷降链 $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$, 都存在正整数 n, 使得当 $i \geqslant n$ 时, 都有 $I_i = I_n$, 则称 R 为左 (右)*Artin 环, *简称* Artin 环.

明显地, 有限环一定是 Artin 环, 但由于整数环 $\mathbf{Z}$ 存在无穷降链

$$(m) \supseteq (2m) \supseteq (2^2 m) \supseteq \cdots,$$

故整数环 $\mathbf{Z}$ 不是 Artin 环.

1970 年, Koh 证明了 R 是 Artin 环 (有单位元) 的充要条件 R 是 Noetehr 环, 并且 R 的每个几乎极大左理想都是极大理想①.

习　题　二

2.1　设环 R 对加法构成一个循环群, 试证明 R 一定是交换环.

2.2　设 a 是环 R 的幂零元, 即存在正整数 n 使得 $a^n = 0$, 试证明 $1 - a$ 是 R 的可逆元.

2.3　设 R 是一个环, 若 R 是布尔环, 即 $a^2 = a$ 对所有的 $a \in R$ 都成立, 试证明 $2a = 0$ 对所有的 $a \in R$ 成立.

① Koh K. On almost maximal right ideals. Proc. Amer. Math. Soc., 1970, 25: 266–272.

2.4 设 R 是一个环, a,b 为 R 中的两个元素, 若 $a+b=ab$ 并且 $1-a$ 有逆元, 试证明 $ab=ba$.

2.5 设 $\mathbf{Q}$ 是有理数环, 试证明 $\mathbf{Q}[\sqrt{2},\sqrt{3}]$ 和 $\mathbf{Q}[\sqrt{2}+\sqrt{3}]$ 相等.

2.6 设 S 是 R 的子环, 若 S 有无穷多个不同的理想, 问 R 是否有无穷多个理想? 证明或给出例子.

2.7 设 R 是实数上的上三角的 3×3 矩阵, 试求 R 的一个理想.

2.8 试求模 6 剩余类环 $\mathbf{Z}_6$ 的所有理想.

2.9 设 S 是交换环 R 中的理想, 若

$$H=\{a\in R|\text{ 存在某个大于等于 1 的正整数 } n,\text{ 使得 } a^n\in S\},$$

试证明 H 也是 R 中的理想.

2.10 设 S,T 是环 R 中的理想, $ST=\left\{\sum_{i=1}^{n}a_ib_i|a_i\in S,b_i\in T,\ n \text{ 为某个正整数}\right\}$, 问 $ST=S\cap T$ 是否一定成立.

2.11 设 S, T 是环 R 中的理想, 试证明 $ST=\left\{\sum_{i=1}^{n}a_ib_i|a_i\in S,b_i\in T,\ n \text{ 为某个正整数}\right\}$ 也是 R 中的理想.

2.12 设 R 是环, $I=\{ab-ba|a,b\in R\}$, 若 I 是左理想, 试证明 I 是 R 中的理想.

2.13 设 R 是环, 若 I 是左理想, $H=\{a\in R|ab=0 \text{ 对所有 } b\in I \text{ 成立 }\}$, 试证明 H 是 R 中的理想.

2.14 设 R 是环, 若 R 只有 $\{0\}$ 和 R 本身是它的左理想, R 没有其他理想, 试证明 R 是可除环.

2.15 设 R 是环, $a\in R, a\neq 0$, 试证明 $I=\{b-ba|b\in R\}$ 是 R 的左理想.

2.16 设 I_1 和 I_2 是环 R 的两个理想, 试证明 $I_1I_2\subseteq I_1\cap I_2$, 并举例说明 I_1I_2 可以真包含在 $I_1\cap I_2$ 内.

2.17　对任意正整数 $n > 1$, 试构造一个阶为 n^2 的非交换环 R.

2.18　试找出 $\mathbf{Z}$ 到自身的一切同态映射, 并求出每一同态的核.

2.19　试证明实数域 $\mathbf{R}$ 与域 $\mathbf{Z}_5$ 是不同构的.

2.20　试证明环 $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ 与环 $\mathbf{Z}_4$ 不是同构的.

2.21　对任意环 R, 试证明存在唯一的环同态 $f : \mathbf{Z} \to \mathbf{R}$.

2.22　设 R_1 和 R_2 是环, $f : R_1 \to R_2$, 对任意 $a, b \in R_1$, 有 $f(a+b) = f(a)+f(b)$, 试证明 $f(a-b) = f(a) - f(b)$ 对任意 $a, b \in R_1$ 都成立.

2.23　设 $\mathbf{Q}$ 是有理数域, 试证明域

$$\mathbf{Q}(\mathrm{i}) = \{a + b\mathrm{i} | a, b \in \mathbf{Q}\}$$

有且只有两个自同构.

2.24　试证明有理数域 $\mathbf{Q}$ 的自同构只有恒等同构.

2.25　设 R 是有限交换环, 若 I 是素理想, 试证明 I 必是极大素理想.

2.26　设 R 是交换整环, m 和 n 为互素的正整数, $a, b \in R$, 若 $a^m = b^m, a^n = b^n$, 试证明 $a = b$.

2.27　设 R 是交换环, 若 $I = \{a \in R |$ 存在某个正整数 n, 使得 $a^n = 0\}$, 试证明 I 是 R 的理想.

2.28　在整数环 $\mathbf{Z}$ 中, 若 p 为素数, 问 (p^2) 和 $(2p)$ 是不是素理想.

2.29　试给出环 $\mathbf{Z}[a + b\sqrt{2}]$ 的一个范数.

2.30　任意环 R 都存在拓扑 τ, 使得 R 成为拓扑环吗?

～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～

伽罗瓦 (E. Galois) 于 1811 年 10 月 25 日出生在法国巴黎郊区拉赖因堡伽罗瓦街的第 54 号房屋内. 伽罗瓦童年时代就表现出有才能、认真、热心等良好的品格. 1770 年, 拉格朗日精心分析了二次、三次、四次方程根式解的结构之后, 提出了方程的预解式概念, 并且还进一步看出预解式和方程的各个根在排列置换下的形式不变性有关, 这时他认识到求解一般五次方程的代数方法可能不存在. 此后, 挪威

数学家阿贝尔利用置换群的理论, 给出了高于四次的一般代数方程不存在代数解的证明. 伽罗瓦通过改进数学家拉格朗日的思想, 把预解式的构成同置换群联系起来的思想, 并在阿贝尔研究的基础上, 进一步发展了他的思想, 把全部问题转化或归结为置换群及其子群结构的分析. 伽罗瓦把代数方程可解性问题转化为与方程相关的置换群及其子群性质的分析问题, 他最主要的成就是提出了群的概念, 用群论彻底解决了代数方程的可解性问题. 人们为了纪念他, 把用群论的方法研究代数方程根式解的理论称之为伽罗瓦理论. 伽罗瓦的工作主要基于两篇论文 ——"关于方程根式解的条件" 和 "用根式求解的本原方程". 在这些论文中, 伽罗瓦将其理论应用于代数方程的可解性问题, 由此引入了群论的一系列重要概念. 在 "关于方程代数解法论文的分析" 中, 伽罗瓦提出了一个重要定理 (未加证明): 一个素数次方程可用根式求解的充要条件是这个方程的每个根都是其中两个根的有理函数.

学习指导

2.1 基本概念

基本要求

(1) 弄清楚环与子环的定义. 熟练掌握整数环, 数域上的多项式环, $n \times n$ 矩阵环和 $[0,1]$ 上连续函数全体构成的环 $C[0,1]$.

(2) 掌握整环和可除环的定义和性质.

(3) 四元数可除环是一类很重要的环.

释疑解难

1. 环与子环的定义相关问题.

(1) 在不同的书中, 环的定义有所不同, 有的书的环不要求含有单位元 1, 但由于这种没有单位元的 "环" 一定可以嵌入到有单位元的环内, 并且很多环的主要结果都只对有单位元的环才成立, 因此本书中的环要求含有单位元. 但环的定义要不要求含有单位元 1 不会对环论本身有影响, 只是有些定理的表达有区别.

(2) 要注意在环 R 中, 由于 R 是一个半群, 故对任何 $a, b \in R$, 有 $ab \in R$ 成立.

(3) 在含有不止一个元的环 R 中, R 是否有可能构成一个乘法群? 由于对 $0 \in R$, 0 没有逆元, 故 R 不可能构成一个乘法群.

(4) 在含有不止一个元的环 R 中, $R^* = R\backslash\{0\}$ 是否一定构成一个乘法群? 这是可能的, 如实数环中的非零元全体就构成了乘法群, 但对于整数环 $\mathbf{Z}$, 大于 1 的元素没有逆元, 因此非零元全体不能构成一个乘法群.

(5) 环的全体可逆元构成一个群.

2. 左零因子与右零因子的区别.

(1) 环 R 中的零元不是零因子.

(2) 如果环 R 有左零因子, 则 R 也必然有右零因子. 反之亦然. 但环中一个元如果是一个左零因子, 则它不一定就是一个右零因子. 反之, 一个右零因子也不一定是一个左零因子.

例如, 在实数域上的所有形如 $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ 的 2×2 矩阵构成的环中, $a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ 是左零因子, 但存在 $b = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, 使得 $ba = 0$, 因此它不是右零因子.

3. 整环与可除环的区别

(1) 对于所有的环 R, 都有 $0u = 0, a0 = 0$, 但 $au = 0$ 时, 不一定有 $u = 0$ 或 $a = 0$.

(2) 整环是指非零环 R 中任何两个非零元的乘积都不等于零, 可除环是指非零环 R 的任何一个非零元的逆元存在. 可除环一定是整环, 但整环不一定是可除环.

(3) 对于整环 R, 当 $au = 0$ 时, 一定有 $u = 0$ 或 $a = 0$. 对于可除环 R, 当方程 $a \neq 0, au = b$ 时, 一定有解 $u = a^{-1}b$. 当然, 对于可除环 R, 当 $au = 0$ 时, 也一定有 $u = 0$ 或 $a = 0$.

2.2　理想和商环

(1) 弄清楚左理想、右理想和理想的定义.

(2) 弄清楚商环、单环和主理想的定义.

(3) 设 R 是交换环, S 是 R 的一个非空子集, 则

$$(S)=\{a_1u_1+\cdots+a_nu_n|a_1,\cdots,a_n\in R,u_1,\cdots,u_n\in S\}.$$

$$(a)=\{ar|r\in R\}.$$

(4) 两个理想的和与积还是理想.

释疑解难

(1) 关于理想的乘法：若 I, J 是环 R 中两个理想, 则 $\{ab|a\in I,b\in J\}$ 不一定是 R 的理想. 但 $\left\{\sum_{i=1}^{n}a_ib_i|a_i\in I,b_i\in J,\ n\text{ 为某个正整数}\right\}$ 一定是 R 的理想, 因此将它规定为理想 I 和理想 J 的乘积, 仍然用记号 IJ 来表示, 因此一定要注意不要将它与 $\{ab|a\in I,b\in J\}$ 混淆. 不过当 I 为主理想时, 则理想 I 和理想 J 的乘积就是 $\{ab|a\in I,b\in J\}$.

(2) 若 I 是环 R 的理想, 则一定有 $RI=I$.

(3) 若环 R 不是交换的, $a\in R$, 则 $Ra=\{ba|b\in R\}$ 是 R 的左理想, 但不一定是右理想, 甚至 $aR\cup Ra$ 也不一定是 R 的理想.

2.3 环的同态

环的同态、同构定理与群的同态、同构定理比较类似, 定理的条件和结论也很类似, 证明方法也基本相同, 区别只在于把正规子群换为理想.

2.4 域

1. 域的基本性质.

(1) 域 F 的理想只有 $\{0\}$ 和 F 本身.

(2) 两个域之间的同态一定是个单同态.

(3) 掌握分式域的形式和定义.

2. 极大理想与素理想的定义和区别.

(1) 极大理想是指 I 是环 R 的一个理想, $I\neq R$, 在 I 和 R 之间没有其他理想.

素理想是指 I 是 R 的理想, 并对任意的 $a,b\in R$, 当 $ab\in I$ 时, 一定有 $a\in I$ 或 $b\in I$.

(2) 判别法：若 R 是交换环, 则 R/I 是一个域当且仅当 I 是 R 的一个极大理想, R/I 是一个整环当且仅当 I 是 R 的一个素理想.

(3) 交换环 R 的极大理想一定是素理想, 反过来, 交换环 R 的素理想不一定是极大理想.

2.5　环上的微分

了解环 R 可以像数学分析一样建立抽象的微分, 知道环上微分的基本性质.

2.6　拓扑环

了解拓扑环的定义, 初步知道环与拓扑的联系, 这部分只供扩展阅读用.

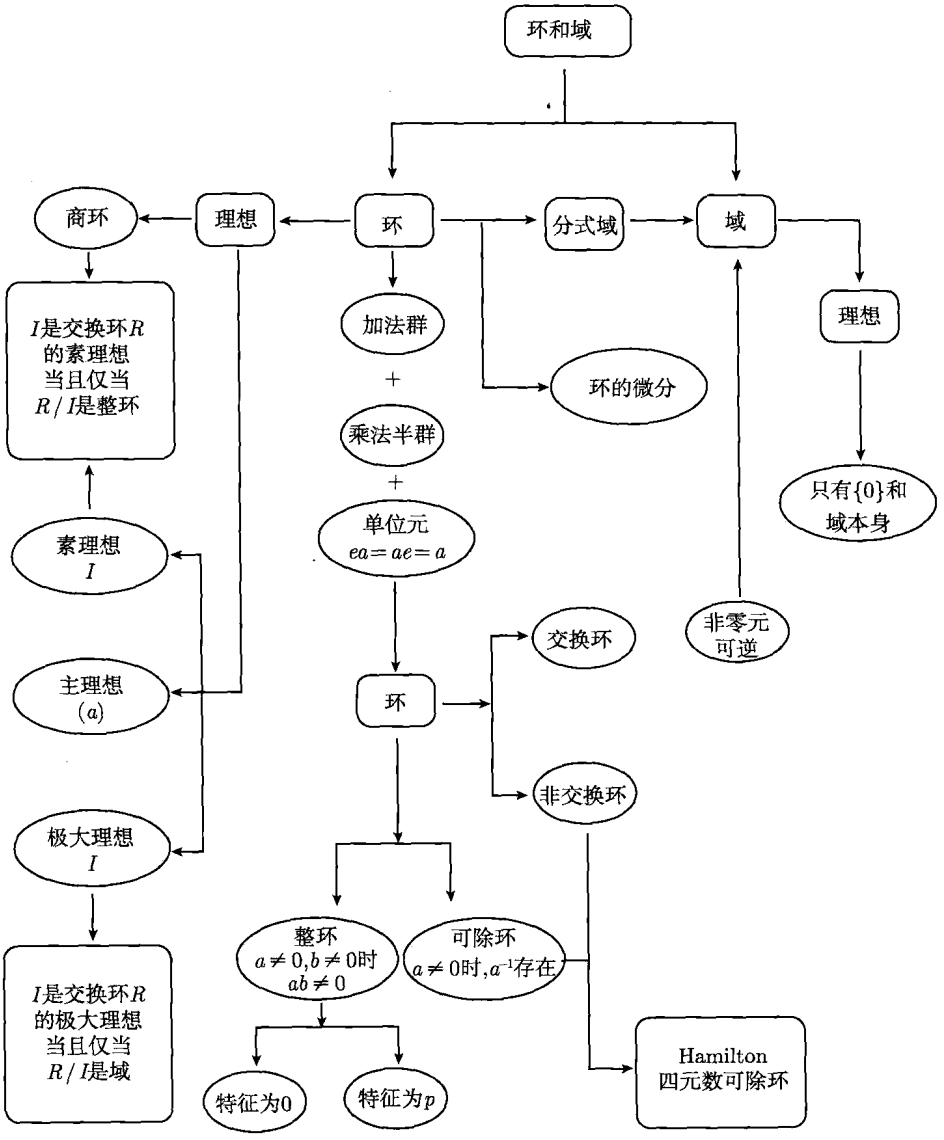
解题技巧

1. 利用理想的性质来解题.

2. 极大理想和素理想的判定.

3. 利用环同构 $f(0)=0, f(1)=1$ 的特点来解题.

知识点联系图


环和域
商环
理想
环
分式域
域
I是交换环R的素理想当且仅当R/I是整环
加法群
+
乘法群
+
单位元
$ea=ae=a$
环的微分
理想
只有{0}和域本身
素理想
I
主理想
(a)
极大理想
I
非零元可逆
交换环
环
非交换环
I是交换环R的极大理想当且仅当R/I是域
整环
$a\neq 0,b\neq 0$时
$ab\neq 0$
可除环
$a\neq 0$时,a^{-1}存在
特征为0
特征为p
Hamilton四元数可除环

第 3 章　环上的多项式

上帝创造了整数, 其他一切都是人造的.

Kronecker (1823-1891, 德国数学家)

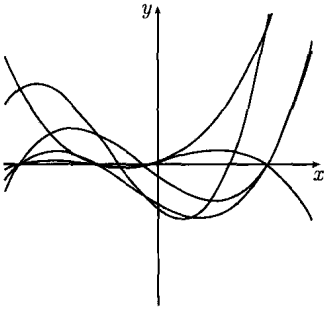
多项式的研究起源于代数方程求解, 是最古老数学问题之一. 在高等代数中已经讨论了数域上的多项式. 实际上, 同样可以定义任意域上的多项式, 也可以在环上研究多项式. 有限域上的多项式在通信、系统工程和计算机科学等许多领域都有非常广泛的应用.

3.1　多　项　式

实数上的多项式函数, 具有下图那样的几何图形, 是一类重要的常用函数, 它的性质是比较容易掌握的.

1　多项式的定义

与域上的多项式一样, 可以定义环上的多项式.



定义 3.1.1　设 R 是一个交换环, 表达式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

称为 R 上的一个多项式 (polynomial), 这里 a_n, a_{n-1}, $\cdots$, a_1, $a_0\in R$, x 与 R 中的元都可交换, 并且 $1x=x$.

对于多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

若 $a_n\neq 0$, a_nx^n 称为该多项式的**首项**, a_n 称为**首项系数** (leading coefficient), 此时称多项式 $f(x)$ 的次数为 n, 首项系数 a_n 为 1 的多项式称为**首一多项式**, x 称为**不定元**(或**变量**), a_0 称为**常数项** (constant term).

R 上以 x 为不定元的多项式全体所构成的集合记作 $R[x]$, $R[x]$ 中两个多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 与 $g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$ 相等是指对应的系数 a_i 和 $b_i(i=0,1,2,\cdots,n)$ 都相等.

2 多项式的运算

多项式之间可以按通常的方式定义加法、减法和乘法等. 对于多项式 $f(x)$, $g(x)\in R[x]$.

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0.$$

令

$$f(x)+g(x)=\sum_{k=0}^{l}(a_k+b_k)x^k,$$

这里 $l=\max\{m,n\}$, 当 $k>n$ 时, 取 $a_k=0$, 当 $k>m$ 时, 取 $b_k=0$.

$$f(x)g(x)=\sum_{k=0}^{m+n}c_kx^k,$$

这里 $c_k=\sum\limits_{i+j=k}a_ib_j$.

直接验算可知, 它们满足交换律、结合律、分配律等, 因此 $R[x]$ 对上面的加法和乘法构成一个交换环, 称为 R 上的**多项式环** (polynomial ring).

定理 3.1.1 *若 R 是一个交换环, 则 $R[x]$ 是一个交换环.*

定义 3.1.2 *设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in R[x]$, 对于 $a\in R$, 定义*

$$f(a)=a_na^n+a_{n-1}a^{n-1}+\cdots+a_1a+a_0,$$

称 $f(a)$ 为 $f(x)$ 在 a 处的值. 若 $f(a)=0$, 就称 a 为 $f(x)$ 在交换环 R 的一个根 (root)(*或零点*).

例 3.1.1 在高等代数中的一元多项式就是实数域 $\mathbf{R}$ 上的多项式.

例 3.1.2 设 $f(x),g(x)\in\mathbf{Z}_3[x]$, 并且

$$f(x)=\overline{2}x^2+x+\overline{1},\quad g(x)=x^5+\overline{2}x+\overline{2},$$

则

$$f(x)+g(x)=(\overline{0}+\overline{1})x^5+(\overline{2}+\overline{0})x^2+(\overline{1}+\overline{2})x+(\overline{1}+\overline{2})$$

$$
\begin{aligned}
&= x^5 + \overline{2}x^2 + \overline{0}x + \overline{0} \\
&= x^5 + \overline{2}x^2, \\
f(x)g(x) &= (\overline{2}x^2 + x + \overline{1})(x^5 + \overline{2}x + \overline{2}) \\
&= \overline{2}x^7 + x^6 + x^5 + \overline{4}x^3 + (\overline{4} + \overline{2})x^2 + (\overline{2} + \overline{2})x + \overline{2} \\
&= \overline{2}x^7 + x^6 + x^5 + x^3 + x + \overline{2},
\end{aligned}
$$

$$
f(\overline{1}) = \overline{2} \cdot \overline{1}^2 + \overline{1} + \overline{1} = \overline{1},
$$

$$
g(\overline{2}) = \overline{2}^5 + \overline{2} \cdot \overline{2} + \overline{2} = \overline{2} + \overline{1} + \overline{2} = \overline{2}.
$$

在高等代数中, 数域 F 上的多项式 $f(x)$ 与多项式 $g(x)$ 相等的充要条件是它们看做 F 的函数时相等.

思考题 3.1.1　交换整环 R 上的多项式 $f(x)$ 与多项式 $g(x)$, 如果对任意的 $a \in R$, $f(a)$ 与 $g(a)$ 都相等, 那么多项式 $f(x)$ 与 $g(x)$ 是相同的多项式吗?

实际上, 在 $\mathbf{Z}_3[x]$ 中, 令 $f(x) = x^5 + \overline{2}x, g(x) = x^3 + \overline{2}x$, 则 $f(\overline{0}) = g(\overline{0}) = \overline{0}$, $f(\overline{1}) = g(\overline{1}) = \overline{0}, f(\overline{2}) = g(\overline{2}) = \overline{0}$, 因此对任意 $a \in \mathbf{Z}_3$, 两个多项式的值相等, 但 $f(x)$ 与 $g(x)$ 是不同的多项式.

3　多项式的性质

性质 3.1.1　设 R 是一个交换整环, $f(x), g(x) \in R[x]$, 则

(1) $\deg(fg) = \deg(f) + \deg(g)$;

(2) $R[x]$ 是一个交换整环;

(3) 若 $c \in R, c \neq 0$, 则 $\deg(cf(x)) = \deg(f)$ 对任意 $f(x) \in R[x]$ 成立;

(4) $\deg(f \pm g) \leqslant \max(\deg(f), \deg(g))$.

思考题 3.1.2　设 R 是一个交换环, $f(x), g(x) \in R[x]$, 则

$$
\deg(fg) = \deg(f) + \deg(g)
$$

是否一定成立呢?

不一定. 这也是一般都只在交换整环上讨论多项式的一个原因. 容易知道, 若 R 是一个交换环, 则只要 $f(x)$ 和 $g(x)$ 的首项系数不是 R 中的零因子, 则 $\deg(fg) = \deg(f) + \deg(g)$ 成立.

性质 3.1.2 若 F 是特征为 $p(p>0, p$ 为素数) 的域, 则对任意多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x],$$

有

$$[f(x)]^p=a_n^px^{pn}+a_{n-1}^px^{p(n-1)}+\cdots+a_1^px^p+a_0^p.$$

证明 由于对任意 $a_n\in F$ 和任意多项式 $g(x)\in F[x]$, 有

$$[a_nx^n+g(x)]^p=(a_nx^n)^p+\sum_{i=1}^{p-1}C_p^i(a_nx^n)^{p-i}[g(x)]^i+[g(x)]^p.$$

由于域 F 的特征为 p, 故除了 $(a_nx^n)^p$ 和 $[g(x)]^p$, 中间项的系数都是 0, 故

$$[a_nx^n+g(x)]^p=(a_nx^n)^p+[g(x)]^p.$$

对于 $g(x)$, 用同样的方法, 可以证明当 $g(x)=a_{n-1}x^{n-1}+h(x)$ 时, 有

$$[g(x)]^p=a_{n-1}^px^{p(n-1)}+h(x)^p.$$

所以, 容易知道 $[f(x)]^p=a_n^px^{pn}+a_{n-1}^px^{p(n-1)}+\cdots+a_1^px^p+a_0^p$. ■

例 3.1.3 在 $\mathbf{Z}_7[x]$ 中, 有 $(x+\overline{1})^7=x^7+\overline{1}$ 和 $(x^2+x+\overline{1})^7=x^{14}+x^7+\overline{1}$.

4 环上的幂级数

在数学分析中, 级数的定义都需要用到收敛性, 环没有收敛的概念, 但还是可以定义形式上的幂级数.

定义 3.1.3 设 R 是一个交换环, 表达式

$$a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n+\cdots$$

称为 R 上的一个形式幂级数 (formal power series), 这里 $a_i\in R(i=0,1,2,\cdots)$, x 与 R 中的元都可交换, R 上的幂级数全体记为 $R[[x]]$.

用与多项式一样的方法可以定义幂级数的加法和乘法, 容易验证, 若 R 是一个交换环, 则 $R[[x]]$ 也是交换环.

定理 3.1.2 若 R 是一个交换环, 则

(1) $R[[x]]$ 是交换环.

(2) 若 R 是交换整环, 则 $R[[x]]$ 是交换整环.

(3) $R[x]$ 是 $R[[x]]$ 的子环.

5　多变量多项式

类似于单变量的多项式, 可以定义多个变量的多项式.

定义 3.1.4　设 R 是一个交换整环, $x_1, x_2, \cdots, x_n$ 是一组未定元, 表达式 $cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 称为一个单项式, 其中 c 是 R 中一个非零元, $k_1, k_2, \cdots, k_n$ 是非负整数.

命题 3.1.1　对于固定的不定元 $x_1, x_2, \cdots, x_n$, 有限多个单项式的和及 0 称为 (这组不定元的) 多项式, 它们全体所构成的集合记作 $R[x_1, x_2, \cdots, x_n]$, 多项式的加减乘法按通常的法则进行, 在这些运算下 $R[x_1, x_2, \cdots, x_n]$ 构成一个交换环.

可以把 $R[x_1, x_2, \cdots, x_n]$ 看成是环 $R[x_1, x_2, \cdots, x_{n-1}]$ 上以 x_n 为变量的单变量多项式环, 也就是说 $R[x_1, x_2, \cdots, x_n] = B[x_n]$, 其中 $B = R[x_1, x_2, \cdots, x_{n-1}]$. 这样通过数学归纳法便可证明 $R[x_1, x_2, \cdots, x_n]$ 是一个交换整环, 称为 R 上的多元 (或多变量) 多项式交换整环, 也可简称多项式环.

定义 3.1.5　单项式 $cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 的次数规定为 $k_1 + k_2 + \cdots + k_n$, 非零多项式的次数定义为构成它的单项式的次数的最大值, 多项式 0 的次数规定为 $-\infty$, 多项式 $f(x_1, x_2, \cdots, x_n)$ 的次数记作 $\deg(f)$.

在多变量的多项式环上, 还可以讨论对称多项式等, 环上的对称多项式与数域上的对称多项式有着类似的结果.

3.2　带余除法

对于实数域上的多项式 $f(x) = x^3 + 1$, $g(x) = x^2 + x + 1$, 一定有 $q(x) = x - 1$, 使得 $f(x) = q(x)g(x) + 2$. 类似地, 环上的多项式也有一样的结论.

1　带余除法

定理 3.2.1　设 R 是一个交换环, $f(x), g(x) \in R[x]$. 若 $g(x) \neq 0$ 且它的首项

系数是 R 中的乘法可逆元, 则存在唯一的一对多项式 $q(x), r(x) \in R[x]$, 使得

(1) $f(x) = g(x)q(x) + r(x)$;

(2) $\deg(r) < \deg(g)$.

此时 $q(x)$ 称为商, $r(x)$ 称为余式.

证明 如果 $\deg(g) > \deg(f)$, 则可取 $q(x) = 0, r(x) = f(x)$.

如果 $\deg(g) \leqslant \deg(f)$, 假设 $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, 这里 $a_n \neq 0, b_m \neq 0, n \geqslant m$, 并且 b_m 可逆.

对多项式 $f(x)$ 次数 n 用归纳法来证明.

① 当 $n = 0$ 时, 则 $m = 0$, 故 $f(x) = a_0, g(x) = b_0$, 由于 $g(x)$ 的首项系数是 R 中的乘法可逆元, 可令 $q = b_0^{-1}a_0$, $r = 0$, 则 $\deg(r) < \deg(g)$, 并且

$$g(x)q(x) + r(x) = b_0(b_0^{-1}a_0) = a_0 = f(x),$$

因此对于 $n = 0$, 结论成立.

② 假设对于每个次数小于 n 的多项式, 结论都是成立的.

③ 对于次数等于 n 的多项式 $f(x) = \sum_{i=0}^{n} a_i x^i$, 容易知道

$$(a_n b_m^{-1} x^{n-m}) g(x) = \sum_{i=0}^{m} (a_n b_m^{-1}) b_i x^{i+n-m}$$

的次数为 n, 并且首项系数为 a_n. 故 $f(x) - (a_n b_m^{-1} x^{n-m}) g(x)$ 是次数小于 n 的多项式. 由归纳假设, 存在多项式 $u(x), r(x) \in R[x]$, 使得

$$f(x) - (a_n b_m^{-1} x^{n-m}) g(x) = u(x)g(x) + r(x),$$

并且 $\deg(r) < \deg(g)$. 令 $q(x) = a_n b_m^{-1} x^{n-m} + u(x)$, 则

$$f(x) = (a_n b_m^{-1} x^{n-m}) g(x) + u(x)g(x) + r(x) = q(x)g(x) + r(x).$$

下面再证明唯一性. 假设 $f(x) = q_1(x)g(x) + r_1(x), f(x) = q_2(x)g(x) + r_2(x)$, 这里 $\deg(r_1) < \deg(g), \deg(r_2) < \deg(g)$, 则 $(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$. 由于

$g(x)$ 的首项系数是 R 中的乘法可逆元, 故 $\deg(q_1(x)-q_2(x))g(x) \geqslant \deg(g(x))$, 但 $\deg(r_2(x)-r_1(x)) < \deg(g(x))$, 因此 $q_1(x)-q_2(x)=0$, 因而 $r_2(x)-r_1(x)=0$, 所以 $f(x)=g(x)q(x)+r(x)$ 中的 $q(x)$ 和 $r(x)$ 是唯一的. ■

2　整除的性质

定义 3.2.1　设 R 是一个交换环, $f(x), g(x) \in R[x]$. 若 $f(x) \neq 0$ 且存在 $h(x) \in R[x]$, 使得 $g(x)=f(x)h(x)$, 则称 $f(x)$ 整除 $g(x)$, 记作 $f(x)|g(x)$ 或 $f|g$.

下面是环上多项式一些基本的性质.

性质 3.2.1　设 R 是一个交换整环, 则

(1) R 中任何一个乘法可逆元整除任何一个多项式;

(2) 任何一个非零多项式整除 0 多项式;

(3) 0 不能整除任何多项式;

(4) 若 $g(x)|f(x), g(x)|h(x)$, 则对任何多项式 $a(x), b(x)$ 都有

$$g(x)|[a(x)f(x)+b(x)h(x)].$$

(5) 若 $g(x)|f(x)$, 且 $f(x) \neq 0$, 则 $\deg(g) \leqslant \deg(f)$;

(6) 若 $g(x)|f(x)$, 则 $g(h(x))|f(h(x))$.

性质 3.2.2　设 R 是一个交换环, $f(x), g(x) \in R[x]$, $g(x) \neq 0$, $g(x)$ 的首项系数是 R 中的乘法可逆元, 则 $g(x)|f(x)$ 当且仅当 $f(x)$ 被 $g(x)$ 除的余式等于零.

3　余数定理

定理 3.2.2　设 R 是交换环, $f(x) \in R[x]$, 则对任意的 $a \in R$, 存在唯一的 $q(x) \in R[x]$, 使得 $f(x)=q(x)(x-a)+f(a)$.

证明　明显地, 若 $f=0$, 则取 $q=0$ 即可.

若 $f \neq 0$, 则存在唯一的一对多项式 $q(x), r(x) \in R[x]$, 使得

$$f(x)=q(x)(x-a)+r(x),$$

并且 $\deg(r(x)) < \deg(x-a) = 1$, 因此 $r(x)$ 是常数多项式 r. 若 $q(x) = \sum_{j=0}^{n-1} b_j x^j$, 则

$$\begin{aligned} f(x) &= q(x)(x-a) + r \\ &= -b_0 a + \sum_{k=1}^{n-1} (-b_k a + b_{k-1}) x^k + b_{n-1} x^n + r. \end{aligned}$$

因此

$$\begin{aligned} f(a) &= -b_0 a + \sum_{k=1}^{n-1} (-b_k a + b_{k-1}) a^k + b_{n-1} a^n + r \\ &= -\sum_{k=0}^{n-1} b_k a^{k+1} + \sum_{k=1}^{n} b_{k-1} a^k + r \\ &= 0 + r = r. \end{aligned}$$

所以, $f(x) = q(x)(x-a) + f(a)$. ■

从证明中可以看出, 事实上, 定理 3.2.1 和定理 3.2.2 对于非交换环也是成立的.

性质 3.2.3 设 R 是交换环, $f(x) \in R[x]$, 则 $a \in R$ 是 $f(x)$ 的根当且仅当 $(x-a) | f(x)$.

定理 3.2.3 设 R 是交换整环, $f(x)$ 是 $R[x]$ 的 n 次多项式 $n \geqslant 1$, 则对 $k \leqslant n$, $a_1, a_2, \cdots, a_k \in R$ 是 $f(x)$ 的不同根当且仅当 $(x-a_1)(x-a_2)\cdots(x-a_k) | f(x)$.

证明 由于 $a_1 \in R$ 是 $f(x)$ 的根, 故存在 $q_1(x)$, 使得 $f(x) = q_1(x)(x-a_1)$, 因此

$$f(a_2) = q_1(a_2)(a_2 - a_1).$$

由 $a_2 - a_1 \neq 0$ 和 R 是整环可知, $q_1(a_2) = 0$, 因此同样可知有 $q_2(x)$, 使得 $q_1(x) = q_2(x)(x-a_2)$. 容易知道可以证明 $(x-a_1)(x-a_2)\cdots(x-a_k) | f(x)$.

反过来, 若 $(x-a_1)(x-a_2)\cdots(x-a_k) | f(x)$, 则明显地, $a_1, a_2, \cdots, a_k \in R$ 是 $f(x)$ 的根. ■

推论 3.2.1 设 R 是交换整环, $f(x)$ 是 $R[x]$ 的 n 次多项式 $n \geqslant 1$, 则 $f(x)$ 在 R 中最多只有 n 个不同根.

证明 若 $a_1, a_2, \cdots, a_k \in R$ 是 $f(x)$ 的不同根, 则 $(x-a_1)(x-a_2)\cdots(x-a_k) | f(x)$, 因此 $\deg((x-a_1)(x-a_2)\cdots(x-a_k)) \leqslant \deg(f(x))$, 所以 $f(x)$ 在 R 中最多只有 n 个不同根. ■

思考题 3.2.1　设 R 是交换环, 但不是整环, $f(x)$ 是 $R[x]$ 的 n 次多项式 $n \geqslant 1$, 则 $f(x)$ 在 R 中最多只有 n 个不同根吗?

不一定. 事实上, 对于交换环 $\mathbf{Z}_8$, $f(x) = x^2 - \overline{1} \in \mathbf{Z}_8[x]$ 是 2 次多项式, 但它有 4 个根 $\overline{1}, \overline{3}, \overline{5}$ 和 $\overline{7}$.

若交换整环 R 上的多项式 $f(x)$ 与多项式 $g(x)$, 如果对任意的 $a \in R$, $f(a)$ 与 $g(a)$ 都相等, 则多项式 $f(x)$ 与 $g(x)$ 不一定是相同的多项式. 不过如果 R 是无限域, 则 $f(x)$ 与 $g(x)$ 一定是相同的.

推论 3.2.2　无限域 R 上的多项式 $f(x)$ 与多项式 $g(x)$, 如果对任意的 $a \in R$, $f(a)$ 与 $g(a)$ 都相等, 那么多项式 $f(x)$ 与 $g(x)$ 一定是相同的多项式.

证明　假如对任意的 $a \in R$, $f(a)$ 与 $g(a)$ 都相等, 但多项式 $f(x)$ 与 $g(x)$ 是不相同的多项式. 令 $h(x) = f(x) - g(x)$, 则 $h(x)$ 是非零多项式, 因此它的次数小于等于 $\max(\deg(f), \deg(g))$, 记为 n, 则由上面推论 3.2.1 可知, $h(x)$ 最多只有 n 个根, 但对任意的 $a \in R$, $h(a) = f(a) - f(a) = 0$, 所以 $f(x) = g(x)$.

从上面的证明过程可以看出, 实际上对于有限域或无限域, 都有下面的结论成立.

推论 3.2.3　域 R 上的 n 次多项式 $f(x)$ 与多项式 $g(x)$, 若存在 $n+1$ 个不同的 $a_i \in R (i = 1, 2, \cdots, n+1)$, 使得 $f(a_i)$ 与 $g(a_i)$ 都相等, 则多项式 $f(x)$ 与 $g(x)$ 一定是相同的多项式.

性质 3.2.4　设 R 是一个交换整环, $f(x), g(x)$ 都是非零多项式. 若 $f(x) | g(x)$ 且 $g(x) | f(x)$, 则 $f(x) = cg(x)$, 其中 c 是一个 R 中的一个乘法可逆元.

证明　设 $f(x) = g(x)a(x)$,$g(x) = f(x)b(x)$, 则 $f(x) = f(x)b(x)a(x)$. 由于 $R[x]$ 是交换整环, 故由 $f(x)(1 - b(x)a(x)) = 0$ 可知, $a(x)b(x) = 1$, 因此 $\deg(a(x)) \leqslant 0, \deg(b(x)) \leqslant 0$, 所以 $a(x)$, $b(x) \in R$ 是 R 中的乘法可逆元. ■

4　域上多项式环的任何理想都是主理想

下面定理是单变量多项式理论的核心定理.

定理 3.2.4　域 F 上的多项式环 $F[x]$ 的任何理想都是主理想.

证明　设 I 是 $F[x]$ 的一个理想. 若 $I = \{0\}$, 则 I 是主理想, 因此只需考虑 $I \neq \{0\}$ 的情形.

在 I 中选一个非零元 $g(x)$, 使多项式 $g(x)$ 的次数是 I 中最小的. 如果 $g(x)$ 的次数是 0, 则 $g(x)$ 是 F 的非零元, 因此 $I = F[x]$ 是主理想.

如果 $g(x)$ 的次数大于 0, 则对任意 $f(x) \in I$. 根据定理 3.2.1, 存在 $q(x), r(x) \in F[x]$, 满足

$$f(x) = q(x)g(x) + r(x),$$

并且 $\deg(r) < \deg(g)$.

由于 $r(x) = f(x) - q(x)g(x) \in I$, 根据 $\deg(g)$ 的极小性, r 一定等于 0, 从而

$$f(x) = q(x)g(x).$$

因此 $f(x)$ 在 $g(x)$ 所生成的主理想中, 所以 I 是 $F[x]$ 的主理想. ■

定义 3.2.2 设 R 是一个交换整环, 若 R 每个理想都是主理想, 则交换整环 R 称为主理想整环 (principal ideal domain).

例 3.2.1 整数环 $\mathbf{Z}$ 和域 F 上的多项式环 $F[x]$ 都是主理想整环.

思考题 3.2.2 主理想整环 R 上的多项式环 $R[x]$ 一定是主理想整环吗?

不一定. 整数环 $\mathbf{Z}$ 是主理想整环, 由于 $\mathbf{Z}[x]$ 的由 2 和 x 生成的理想 $(2, x)$ 不是主理想, 故 $\mathbf{Z}$ 上的多项式环 $\mathbf{Z}[x]$ 不是主理想整环.

思考题 3.2.3 主理想整环 R 上的子环 S 一定是主理想整环吗?

不一定. 实际上, 有理数域 $\mathbf{Q}$ 上的多项式环 $\mathbf{Q}[x]$ 是主理想整环, 但它的子环 $\mathbf{Z}[x]$ 不是主理想整环. 实数域 $\mathbf{R}$ 上的多项式环 $\mathbf{R}[x]$ 是主理想整环, 它的子环 $\mathbf{Q}[x]$ 也是主理想整环.

定义 3.2.3 设 F 是域, $f(x), g(x), h(x), \in F[x]$, 如果 $h(x)|f(x), h(x)|g(x)$, 则 $h(x)$ 称为 $f(x)$ 和 $g(x)$ 的一个公因式.

设 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的一个公因式, 并且对 $g(x), f(x)$ 的任何一个公因式 $h(x)$ 都有 $h(x)|d(x)$, 则 $d(x)$ 称为 $f(x)$ 和 $g(x)$ 的最大公因式 (greatest common divisor), 记作 $\gcd(f(x),\ g(x))$.

性质 3.2.5 设 F 是域, $d_1(x), d_2(x)$ 都是 $f(x), g(x)$ 的最大公因式, 则 $d_1(x) = c \cdot d_2(x)$, 其中 c 是域 F 中的一个非零元.

证明 由于 $d_1(x)|d_2(x), d_2(x)|d_1(x)$, 故 $d_1(x) = c \cdot d_2(x)$. ■

由上面引理可知最大公因式在相差一个常数因子的意义下是唯一的, 因此首项系数都等于 1 的最大公因式是唯一的.

定理 3.2.5　*设 F 是域, $f(x), g(x)$ 不全为零, 则最大公因式 $\gcd(f(x), g(x))$ 存在, 并且存在 $a(x), b(x)$, 使得*

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

证明　令 I 为 $F[x]$ 中由 $f(x)$ 和 $g(x)$ 生成的理想, 根据定理 3.2.4, I 是一个主理想, 任取 I 的一个生成元 $d(x)$. 由于 I 由 $f(x), g(x)$ 生成, 存在 $a(x), b(x) \in R[x]$, 使得

$$d(x) = a(x)f(x) + b(x)g(x).$$

下面只需证明 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的最大公因式就可以了. 根据主理想的定义, $d(x)|f(x), d(x)|g(x)$, 故 $d(x)$ 是 $f(x), g(x)$ 的一个公因式.

设 $h(x)|f(x), h(x)|g(x)$, 则存在 $u(x), v(x) \in F[x]$ 使

$$f(x) = u(x)h(x), \quad g(x) = v(x)h(x).$$

于是

$$d(x) = [a(x)u(x) + b(x)v(x)]h(x),$$

因此 $h(x)|d(x)$, 所以 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的最大公因式. ■

高等代数中学过的辗转相除法可以推广到任意域上, 用它可以计算最大公因式.

例 3.2.2　在 $\mathbf{Z}_{13}[x]$ 中, 设多项式 $f(x) = x^4 + \overline{3}x^3 - x^2 - \overline{4}x - \overline{3}, g(x) = \overline{3}x^3 + \overline{10}x^2 + \overline{2}x - \overline{3}$, 则用辗转相除法可以得到 $f(x)$ 和 $g(x)$ 的最大公因式 $\gcd(f(x), g(x)) = x + \overline{3}$.

定义 3.2.4　*若 $f(x)$ 和 $g(x)$ 的最大公因式 $\gcd(f(x), g(x)) = 1$, 则称 $f(x)$ 和 $g(x)$ 互素.*

推论 3.2.4　*域 F 上的多项式 $f(x)$ 和 $g(x)$ 互素的充要条件是存在 $u(x), v(x) \in F[x]$, 使得 $f(x)u(x) + g(x)v(x) = 1$.*

例 3.2.3　设 $\mathbf{R}[x]$ 为实数域 $\mathbf{R}$ 上的多项式环, $f(x) = x^2+1, g(x) = x^5+x^3+1 \in \mathbf{R}[x]$, 试求 $f(x)$, $g(x)$ 生成的理想.

证明 由于 $f(x)$ 和 $g(x)$ 互素, 故存在 $p(x)$ 和 $q(x)$, 使得

$$p(x)f(x)+q(x)g(x)=1.$$

实际上, 取 $p(x)=-x^3$, $q(x)=1\in R[x]$, 则

$$-x^3(x^2+1)+1(x^5+x^3+1)=1,$$

所以 $f(x)$ 和 $g(x)$ 生成的理想 $(f(x),g(x))=(1)=\mathbf{R}[x]$. ■

5 域上多项式的应用

数字通讯在现代科学技术中起着非常重要的作用, 在计算机之间的数字传递, 最好是没有任何误差, 但在传送信息过程中难免出现误差, 如何解决这一问题呢? 解决这一问题的一个方法是设法判断所接收到的信息是否有错误, 如有错误就要求发送者重新发该信息. 为了便于检验错误, 可先对原信息进行适当的加工, 可以利用环上的多项式进行编码.

设要传送的信息码长度为 k, 信息码为 $b_0,b_1,\cdots,b_{k-1}$, 这里 $b_i\in\mathbf{Z}_2$, 则

$$m(x)=b_0+b_1x+\cdots+b_{k-1}x^{k-1}\in\mathbf{Z}_2[x]$$

称为**信息码多项式**.

又设码词为 $a_0,a_1,\cdots,a_{n-1},a_i\in\mathbf{Z}_2$, 则 $v(x)=a_0+a_1x+\cdots+a_{k-1}x^{n-1}\in\mathbf{Z}_2[x]$ 称为**码词多项式**.

利用域上的多项式, 可以给出一种方法, 将每一个信息码多项式按一定规则得到对应的码词多项式, 从而把每一个信息码变为码词.

先选定一个 $n-k$ 次多次式 $p(x)\in\mathbf{Z}_2[x]$ 作为生成多项式.

若 $m(x)$ 是信息码多项式, 设用 $p(x)$ 整除 $x^{n-k}m(x)$ 所得的余式为 $r(x)$, 即

$$x^{n-k}m(x)=q(x)p(x)+r(x),\quad \deg(r)<\deg(p).$$

令 $v(x)=x^{n-k}m(x)-r(x)$, 则 $p(x)$ 整除 $v(x)$, 则 $v(x)$ 就作为码词多项式, 它的系数就是码词. 这样, 可以将每一个信息码通过以上的多项式运算变为码词.

可用例子来说明上面的过程, 选定一个 $n-k=4$ 次多项式作为生成多项式, 则

生成多项式	$p(x)=\overline{1}+x+x^2+x^3+x^4$
信息码	101
信息码多项式	$m(x)=\overline{1}+\overline{0}x+x^2$
$x^4m(x)$	x^4+x^6
$r(x)$	$\overline{1}+x$
码词多项式 $v(x)$	$\overline{1}+x+\overline{0}x^2+\overline{0}x^3+x^4+\overline{0}x^5+x^6$
码词	1100 101

对每一个信息码都可作以上方法求得对应的码词, 接收者收到码词后, 先写出收到的码词多项式 $v(x)$, 然后检验 $p(x)$ 能否整除 $v(x)$, 若 $p(x)|v(x)$, 则此信息无错, 否则信息有错.

例 3.2.4　设生成多项式为 $p(x)=\overline{1}+x^2+x^3+x^4$, 试验证码词 1011011 和 1100101 有无错.

解　由于 1011011 的码词多项式 $v(x)$ 为 $\overline{1}+x^2+x^3+x^5+x^6$, 并且

$$v(x)=p(x)(x^2+\overline{1})+x^2,$$

故 $p(x)$ 不能整除 $v(x)$, 所以码词 1011011 有错.

由于 1100101 的码词多项式 $v(x)$ 为 $\overline{1}+x+x^4+x^6$, 并且

$$v(x)=p(x)(x^2+x+\overline{1}),$$

故 $p(x)$ 能整除 $v(x)$, 所以码词 1100101 无错.

不过要注意的是, 当收到的码词多项式 $v(x)$ 不能被 $p(x)$ 整除时, 此码词一定有错. 但若 $p(x)$ 能整除 $v(x)$, 这时收到的码词也并非一定无错, 有可能是错误位数多而检查不了, 但这种发生多位错误的概率很小. 在实际中, 还可设计一种专门的电子线路, 无需作任何多项式的运算, 操作员发报时也只需打信息码就可以了, 电子线路会自动转换成由 $p(x)$ 生成的码词, 接收时也有专门电子线路自动检验是否有错, 非常方便和实用.

3.3　因 式 分 解

中学课本上就有了一些具体的方法, 可以将一个多项式进行因公分解, 如将

x^3-1 分解为 $(x-1)(x^2+x+1)$, 但要分解到怎么样才是不能再分解呢? 如在 $\mathbf{Q}(\sqrt{3})$ 中,x^2-3 可以分解为 $(x+\sqrt{3})(x-\sqrt{3})$, 但在整数 $\mathbf{Z}$ 中,x^2-3 就不能再分解了, 容易想到因子分解与多项式的系数所在的环有关, 因此在环中, 要重新定义整除和不可约等基本的一些概念.

1 整除、相伴、素元和不可约元

定义 3.3.1 *设 R 是一个交换整环, $a,b\in R, b\neq 0$, 若存在 $c\in R$, 使 $a=bc$, 则称 b 整除 a, 记为 $b|a$.*

例 3.3.1 在 $\mathbf{Z}_5$ 中, $\overline{2}\cdot\overline{3}=\overline{1}$, 故 $\overline{2}$ 整除 $\overline{1}$.

交换整环中的整除概念是整数环和多项式环中的整除概念的推广.

定义 3.3.2 *当 b 整除 a 时, b 称为 a 的一个因子* (divisor).

在整数环 $\mathbf{Z}$ 中, 如果两个非零整数 a,b 相互整除, 则这两个数的商为 ± 1. 对整环的整除而言, 如果两个因子仅相差一个逆元, 可以认为这两个因子是相同的.

定义 3.3.3 *若环 R 中的两个非零元 a, b 满足 $b|a$, $a|b$, 则称 a 和 b 是相伴元* (associates).

容易看出, 若 R 是交换整环, 则 a 和 b 是相伴的当且仅当存在环 R 中的乘法可逆元 u, 使得 $a=ub$. 不难证明, 相伴是环 R 中一个等价关系.

例 3.3.2 在 $\mathbf{Z}_5$ 中, 由于 $\overline{4}=\overline{2}\cdot\overline{2}$, $\overline{2}=\overline{3}\cdot\overline{4}$, 故 $\overline{2}$ 整除 $\overline{4}$ 且 $\overline{4}$ 整除 $\overline{2}$, 因此 $\overline{2}$ 和 $\overline{4}$ 相伴.

可将整数环 $\mathbf{Z}$ 中, 素数的概念推广为一般交换环的素元.

定义 3.3.4 *设 p 是交换环 R 中的一个非零元, 若 p 不是乘法可逆元, 且 $p=ab$ 时, 一定有 $p|a$ 或 $p|b$, 则称 p 为一个素元* (prime element).

在整数环 $\mathbf{Z}$ 中, 若 p 为素数, $p=ab$, 则一定有 $a=\pm 1$ 或 $b=\pm 1$. 在交换整环 R 中可以根据素数的这个特征将它推广为不可约元.

定义 3.3.5 *设 p 是交换环 R 中的一个非零元, 若 p 不是乘法可逆元, 且 $p=ab$ 时, a 和 b 中一定有一个是乘法可逆元, 则称 p 为一个不可约元* (irreducible element). *若 p 不是不可约元, 则称 p 为一个可约元* (reducible element).

例 3.3.3　在整数 $\mathbf{Z}$ 上的多项式环 $\mathbf{Z}[x]$ 中, 由于 $2x+2=2(x+1)$, 并且 2 和 $x+1$ 都不是可逆元, 故 $2x+2$ 是 $\mathbf{Z}[x]$ 的可约元.

思考题 3.3.1　*设 R 是交换环, R 中的素元一定是不可约元吗?*

交换环 R 中的素元不一定是不可约元, 但交换整环 R 中的素元一定是不可约元. 实际上, 在环 $\mathbf{Z}_6$ 中, $\overline{2}$ 是素元, 由于 $\overline{2}=\overline{2}\cdot\overline{4}$, 但 $\overline{2}$ 和 $\overline{4}$ 都不是 $\mathbf{Z}_6$ 的乘法可逆元, 故 $\overline{2}$ 不是 $\mathbf{Z}_6$ 的不可约元.

性质 3.3.1　*若 R 是交换整环, 则 R 中的素元一定是不可约元.*

证明　若 a 是 R 中的素元, 则 $a=bc$ 时, 一定有 $a|b$ 或 $a|c$, 不妨设存在 d 使得 $b=ad$, 则 $a=adc$. 由于 R 是整环, 故 $dc=1$, 从而 c 是乘法可逆元, 所以素元 a 一定是不可约元. ■

不难验证, 素元生成的理想是素理想.

性质 3.3.2　*若 R 是交换整环, 则 $a\in R$ 是素元的充要条件为 (a) 是非零素理想.*

2　唯一因子分解环

由算术基本定理可知, 任何一个大于 1 的自然数可以唯一地分解成有限多个素数的乘积, 如 $210=2\cdot3\cdot5\cdot7$, 并且适当的置换后, 这种分解是唯一的. 即 a 是大于等于 2 的整数, 则 a 可表示为 $a=p_1\cdots p_r$(其中 $p_1,\cdots,p_r$ 全是素数, r 是一个非负整数). 如果 $a=p_1\cdots p_s=q_1\cdots q_t$(其中 $p_1,\cdots,p_s,q_1,\cdots,q_t$ 全都是是素数), 则 $s=t$, 并且在对 $q_1,\cdots,q_t$ 作适当的更换后每个 p_r 与 q_r 相等.

定义 3.3.6　*交换整环 R 称为唯一因子分解环* (unique factorization domain). *若下面条件满足:*

(1) *R 中任何一个非零元 a 可表示为*

$$a=cp_1\cdots p_r,$$

其中 c 是乘法可逆元, $p_1,\cdots,p_r$ 全是不可约元, r 是一个非负整数.

(2) *设 $cp_1\cdots p_s=dq_1\cdots q_t$, 其中 c,d 是乘法可逆元, $p_1,\cdots,p_s,q_1,\cdots,q_t$ 都是 R 中的不可约元, 则 $s=t$ 并且在对 $q_1,\cdots,q_t$ 作适当的置换后每个 p_r 与 q_r 相伴.*

思考题 3.3.2 在唯一因子分解环的定义中，为什么需要条件 (2)，有可以分解成不可约元的乘积，但分解不唯一的环吗？

有的. 实际上，在交换整环 $\mathbf{Z}[\sqrt{10}]=\{a+b\sqrt{10}|a,b\in\mathbf{Z}\}$ 中，$4+\sqrt{10}$ 和 $4-\sqrt{10}$ 都是 $\mathbf{Z}[\sqrt[4]{10}]$ 的不可约元，2 和 3 也是 $\mathbf{Z}[\sqrt{10}]$ 的不可约元，但对于 $6\in\mathbf{Z}[\sqrt{10}]$，有两个不同的分解 $6=2\cdot 3=(4+\sqrt{10})(4-\sqrt{10})$.

很容易看出下面结论成立.

性质 3.3.3 若 R 是一个唯一因子分解环，$p\in R$ 是一个不可约元，p 整除 ab，则 p 整除 a 或 p 整除 b.

思考题 3.3.3 在唯一因子分解环 R 中，不可约元和素元有区别吗？

没有区别. 在交换整环 R 中，素元一定是不可约元. 唯一因子分解环中的不可约元一定是素元，因此在唯一因子分解环 R 中，可以不再区分素元和不可约元. 在整数环 $\mathbf{Z}$ 中，每个元素都可以唯一分解成素数的乘积，如对 $30\in\mathbf{Z}$，有 $30=2\cdot 3\cdot 5$.

定义 3.3.7 设 R 是交换环，$f(x)\in R[x]$ 是一个非零元，若 $f(x)$ 不是乘法可逆元，且 $f(x)=g(x)h(x)$ 时，$g(x)$ 和 $h(x)$ 中一定有一个是乘法可逆元，则称 $f(x)$ 为多项式环 $R[x]$ 的一个不可约多项式 (irreducible polynomial). 若 $f(x)$ 次数大于零，并且不是多项式环 $R[x]$ 的可约多项式，则称 $f(x)$ 为一个可约多项式 (reducible polynomial).

容易验证，$f(x)=4(x-1)$ 和 $g(x)=x^2-1$ 为整数 $\mathbf{Z}$ 上多项式环 $\mathbf{Z}[x]$ 的可约多项式，但 $h(x)=x^2+1$ 是多项式环 $\mathbf{Z}[x]$ 的不可约多项式.

若 F 是一个域，则 0 次的非零多项式一定是乘法可逆元，因此一个多项式 $f(x)\in F[x]$ 是一个不可约多项式，当且仅当 $\deg(f)>0$，并且 $f(x)$ 不能分解成两个次数小于 $\deg(f)$ 的多项式的乘积. 不过若 R 是环，但 R 不是域，则 $f(x)\in R[x]$，$\deg(f)>0$ 不能分解成两个次数小于 $\deg(f)$ 的多项式的乘积时，$f(x)$ 不一定是 $R[x]$ 的不可约多项式. 事实上，$f(x)=4(x-1)\in\mathbf{Z}[x]$ 不能分解成两个次数小于 1 的多项式的乘积，但它是 $\mathbf{Z}[x]$ 的可约多项式.

定义 3.3.8 若 $f(x)$ 是一个可约多项式，则存在一个多项式 $g(x)$ 满足 $g(x)$ 整除 $f(x)$ 且 $0<\deg(g)<\deg(f)$，$g(x)$ 称为 $f(x)$ 的一个真因式.

引理 3.3.1 设 F 是域，$f(x),g(x)\in F[x]$ 且 $f(x)$ 不可约，若 $f(x)$ 不整除 $g(x)$，则 $\deg(\gcd(f(x),g(x)))=0$.

证明　记 $d(x)=\gcd(f(x),g(x))$, 则存在 $h(x)$ 使 $f(x)=d(x)h(x)$. 由于 $f(x)$ 不可约, $\deg(d)=0$ 或 $\deg(h)=0$. 假如 $\deg(h)=0$, 则 $h(x)$ 是个非零常数 c, 此时 $f(x)=cd(x)$, $d(x)|g(x)$, 从而 $f(x)|g(x)$, 但 $f(x)$ 不整除 $g(x)$, 所以 $\deg(d)=0$. ■

定理 3.3.1　*设 F 是域, $p(x)$ 是一个不可约多项式, $p(x)$ 整除 $f(x)g(x)$, 则 $p(x)|f(x)$ 或 $p(x)|g(x)$.*

证明　如果 $p(x)$ 不整除 $f(x)$, 由上面引理知 $p(x)$ 与 $f(x)$ 互素, 根据定理 3.2.5 存在 $a(x),b(x)\in F[x]$, 使

$$a(x)p(x)+b(x)f(x)=1$$

两边同乘 $g(x)$ 得

$$a(x)p(x)g(x)+b(x)f(x)g(x)=g(x).$$

由于 $p(x)$ 整除 $f(x)g(x)$, 它也整除上式的左边, 所以 $p(x)|g(x)$. ■

推论 3.3.1　*设 F 是域, $p(x)$ 是一个不可约多项式, $p(x)|f_1(x)\cdots f_n(x)$, 则 $p(x)$ 整除某个 $f_i(x)$.*

如何判断一个多项式是否可约是一个重要但比较难的问题. 在高等代数, 有一些方法可以判别多项式是否可约, 如 Eisenstein 判别法, 但不一定总是有效的.

例 3.3.4　设 $f(x)$ 是域 F 上的一个次数等于 2 或 3 的多项式, 试证明 $f(x)$ 在 F 上是可约多项式当且仅当 $f(x)$ 在 F 上有根.

证明　若 $f(x)$ 是 F 上的可约多项式, 则存在 $g(x),h(x)\in F[x]$, 使得 $f(x)=g(x)h(x)$, 并且 $\deg(g)<\deg(f),\deg(h)<\deg(f)$. 由于 $f(x)$ 的次数等于 2 或 3 的多项式, 故 $g(x)$ 和 $h(x)$ 至少有一个是一次因子. 不妨设 $g(x)=ax+b(a\neq 0)$, 则 $-a^{-1}b$ 是 $g(x)$ 的根, 因而 $-a^{-1}b$ 也是 $f(x)$ 的根.

反过来, 若 a 是 $f(x)$ 在 F 的根, 则 $(x-a)|f(x)$, 所以 $f(x)$ 可约. ■

思考题 3.3.4　*设 $f(x)$ 是域 F 上的一个次数大于 3 的多项式, 若 $f(x)$ 在 F 是可约的, 则 $f(x)$ 在 F 上有根吗?*

不一定. 如实数域 $\mathbf{R}$ 上的多项式 $f(x)=x^4+2x^2+1$, 由 $x^4+2x^2+1=(x^2+1)^2$ 可知, 它是可约的, 但 $f(x)$ 在实数域 $\mathbf{R}$ 上没有根.

例 3.3.5　试判别 $f(x)=x^2+\bar{1}$ 在 $\mathbf{Z}_2[x]$ 和 $\mathbf{Z}_3[x]$ 中是否可约.

证明 在 $\mathbf{Z}_2[x]$ 中, 有 $f(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{0}$, 因此 $f(x)$ 在 $\mathbf{Z}_2[x]$ 中可约, 并且 $f(x) = (x + \overline{1})(x + \overline{1})$.

在 $\mathbf{Z}_3[x]$ 中, 有 $f(\overline{0}) = \overline{0}^2 + \overline{1} = \overline{1}$, $f(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{2}$, $f(\overline{2}) = \overline{2}^2 + \overline{1} = \overline{2}$, 因此 $f(x)$ 在 $\mathbf{Z}_3$ 没有根, 所以 $f(x) = x^2 + \overline{1}$ 在中 $\mathbf{Z}_3[x]$ 不可约. ■

下面可以证明 $F[x]$ 是唯一因子分解环了.

定理 3.3.2 设 $f(x)$ 是域 F 上的一个次数大于 0 的多项式, 则

$$f(x) = cp_1(x) \cdots p_n(x),$$

其中 c 是一个非零常数, $p_1(x), \cdots, p_n(x)$ 是首一不可约多项式, 以上等式称为 $f(x)$ 的不可约分解式.

这里的 c 和真因式列 $\{p_1(x), \cdots, p_n(x)\}$ 在相差一个次序的意义下由 $f(x)$ 唯一确定的.

证明 先证明分解式的存在性, 用归纳法对 $\deg(f)$ 进行归纳证明.

(1) 当 $\deg(f) = 1$ 时, $f(x)$ 可写成 $cf_1(x)$(这里 c 是 $f(x)$ 的首项系数), 因此结论成立.

(2) 假设结论对 $\deg(f) < n$ 的 $f(x)$ 都成立.

(3) 下面证明当 $\deg(f) = n$ 时结论也成立.

如果 $f(x)$ 是不可约多项式, 则结论自然成立. 若 $f(x)$ 是可约多项式, 则存在次数小于 $\deg(f)$ 的非零多项式 $f_1(x), f_2(x)$, 使得 $f(x) = f_1(x)f_2(x)$.

由于 $\deg(f_1) < n$, $\deg(f_2) < n$, 故由归纳假设可知 $f_1(x), f_2(x)$ 的分解式存在.

$$f_1(x) = cp_1(x) \cdots p_r(x),$$

$$f_2(x) = c'p_{r+1}(x) \cdots p_n(x),$$

其中 c, c' 是非零常数, $p_1(x), \cdots, p_n(x)$ 是首一不可约多项式. 所以 $\deg(f) = n$ 时结论也成立.

(4) 最后证明分解式的唯一性.

对 $f(x)$ 的因式个数 n 进行归纳证明. 当 $n = 1$ 时, 结论显然成立. 假设分解式在因式个数小于 n 时是唯一的, 则因式个数为 $n(n > 1)$ 时, 若

$$f(x) = c''q_1(x) \cdots q_m(x)$$

是另一个不可约分解式.

由于 $p_i(x), q_n(x)$ 都是首一多项式, c 和 c'' 都等于 $f(x)$ 的首项系数, 故 $c = c''$.

由于 $p_1(x)|f(x)$, 根据推论 3.3.1, $p_1(x)$ 整除某个 $q_j(x)$, 不妨设 $p_1(x)|q_1(x)$. 但是 $q_1(x)$ 也是不可约的, 故 $p_1(x) = q_1(x)$. 因此

$$p_2(x)\cdots p_n(x) = q_2(x)\cdots q_m(x).$$

利用归纳假设得知 $m = n$, 并且真因式列 $\{p_2(x)\cdots p_n(x)\}$ 和 $\{q_2(x)\cdots q_m(x)\}$ 只相差一个次序. ■

推论 3.3.2　*任意域 F 上的单变量多项式环 $F[x]$ 是唯一因子分解环.*

例 3.3.6　试将多项式 $f(x) = x^4 + \overline{1}$ 在 $\mathbf{Z}_3[x]$ 中分解成不可约多项式的乘积.

解　由于 $f(\overline{1}) = \overline{2}$, $f(\overline{2}) = \overline{2}$, 故 $f(x)$ 没有一次因子.

设 $f(x) = (x^2 + ax + b)(x^2 + cx + d)$, 则比较系数可知

$$ad = \overline{1}, \quad a + c = \overline{0}, \quad b + d + ac = \overline{0}, \quad ad + bc = \overline{0}.$$

由 $a + c = \overline{0}$ 和 $ad + bc = \overline{0}$, 可得 $c(b - d) = \overline{0}$. 若 $c = \overline{0}$, 则由 $b + d + ac = \overline{0}$ 可知 $b = -d$, 故由 $ad = \overline{1}$ 可知 $b^2 = -\overline{1}$, 矛盾. 因此 $c \neq \overline{0}$, 故由 $c(b - d) = \overline{0}$ 可知 $b = d$. 由 $a + c = \overline{0}$ 可得 $a = -c$. 因此可取 $a = \overline{1}$, $b = \overline{2}$, $c = \overline{2}$, $d = \overline{2}$, 从而

$$f(x) = (x^2 + x + \overline{2})(x^2 + \overline{2}x + \overline{2}).$$

由于 $g(x) = x^2 + x + \overline{2}$, $h(x) = x^2 + \overline{2}x + \overline{2}$ 在 $\overline{1}$ 和 $\overline{2}$ 都不为零, 故 $g(x)$ 和 $h(x)$ 都没有一次因子, 因而是不可约多项式, 所以 $f(x) = (x^2 + x + \overline{2})(x^2 + \overline{2}x + \overline{2})$.

3　多项式的重因式

$f(x) = cp_1(x)\cdots p_n(x)$ 是 $f(x)$ 的不可约分解式时, 其中的不可约因式 $p_i(x)$ 不一定两两不同, 若将相同的因式写在一起就可将上式改为

$$f(x) = cp_1(x)^{k_1}\cdots p_r(x)^{k_r},$$

这里 $p_1(x), \cdots, p_r(x)$ 是两两不同的首一不可约多项式.

定义 3.3.9 若 $f(x)=cp_1(x)^{k_1}\cdots p_r(x)^{k_r}$, 并且 $p_1(x),\cdots,p_r(x)$ 是两两不同的首一不可约多项式, 则称该分解式为 $f(x)$ 的标准不可约分解式. 指数 k_i 称为因式 $p_i(x)$ 在 $f(x)$ 中的重数 (multiplicity), 重数大于 1 的因式称为重因式.

例 3.3.7 在 $\mathbf{Z}_3[x]$ 中, $f(x)=\overline{2}x^3+\overline{2}x^2+\overline{2}x+\overline{2}$ 的标准不可约分解式为 $f(x)=\overline{2}(x+\overline{1})(x^2+\overline{1})$.

思考题 3.3.5 如何判断多项式 $f(x)$ 有没有重因式呢?

在微积分中, 可以利用导数来判断多项式 $f(x)$ 有没有重因式. 由于

$$f'(x)=\lim_{\Delta x\to 0}\frac{f(x+\Delta x)-f(x)}{\Delta x},$$

故 $(a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0)'=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$. 但在环和域中, 没有了微积分中导数的几何或物理意义, 就无法按上面的方式来定义导数. 不过, 可以按照多项式导数的规律, 来定义多项式的形式导数.

定义 3.3.10 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in F[x]$, 称

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$$

为 $f(x)$ 的导数.

与微积分中的导数类似, 可以证明下面的导数性质仍然成立, 因此容易知道它是多项式环 $F[x]$ 的微分.

性质 3.3.4 对任意 $f(x),g(x)\in F[x]$, 有

$$(f(x)+g(x))'=f'(x)+g'(x),$$

$$(g(x)f(x))'=f'(x)g(x)+f(x)g'(x).$$

在高等代数, 数域上一个非零多项式的导数的次数是原多项式的次数减 1, 因此考虑如下的问题是有必要的.

思考题 3.3.6 交换整环上一个非零多项式的导数的次数一定是原多项式的次数减 1 吗?

例 3.3.8 在 $\mathbf{Z}_5[x]$ 中, $f(x)=\overline{2}x^5+x^2+\overline{2}x+\overline{1}$ 的导数为 $f'(x)=\overline{0}x^4+\overline{2}x+\overline{2}=\overline{2}x+\overline{2}$.

与高等代数数域上一个非零多项式性质类似, 对于特征为 0 的域 F, 有如下的性质成立, 不过该性质对一般的域是不一定成立的.

性质 3.3.5　设 $f(x)=cp_1(x)^{k_1}\cdots p_r(x)^{k_r}$ 是特征为 0 的域 F 上一个次数大于 1 的多项式 $f(x)$ 的标准不可约分解式, 则

$$\gcd(f(x),f'(x))=\prod_{i=1}^{r}p_i(x)^{k_i-1}.$$

下面结果对任意域成立.

性质 3.3.6　设 F 是域, 若 $f(x)\in F[x]$, $\gcd(f(x),f'(x))=1$, 则 $f(x)$ 无重因子.

证明　如果 $f(x)=g(x)^rh(x)$, 其中 $\deg(g)>0, h(x)\neq 0, r>1$, 则

$$\begin{aligned}f'(x)&=rg(x)^{r-1}g'(x)h(x)+g(x)^rh'(x)\\&=g(x)^{r-1}[rg'(x)h(x)+g(x)h'(x)].\end{aligned}$$

因此 $g(x)|\gcd(f(x),f'(x))$, 从而 $g(x)=1$, 所以 $f(x)$ 无重因子. ■

定义 3.3.11　设 R 是整环, $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in F[x]$, $a\in R$, 若 $(x-a)^k$ 整除 $f(x)$, 但 $(x-a)^{k+1}$ 不能整除 $f(x)$, 则称 a 为 $f(x)$ 的 k 重根.

性质 3.3.7　设 R 是整环, $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in F[x]$, $a\in R$ 是 $f(x)$ 的重根当并且仅当 a 是 $f(x)$ 和 $f'(x)$ 的根.

3.4　本原多项式

在高等代数中, 如果一个整数系数的非零多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 的系数没有异于 ±1 的公因子, 那么就称之为本原多项式, 如整数系数多项式 $f(x)=x^3+2x^2+3$ 是本原多项式.

1　本原多项式的定义

定义 3.4.1　设 R 为环, $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个非零多项式, 其中 $a_n,a_{n-1},\cdots,a_1,a_0\in R$. 如果除了乘法可逆元外, $a_n,a_{n-1},\cdots,a_1,a_0$ 没有其他公因子, 则称 $f(x)$ 为一个本原多项式 (primitive polynomial).

例 3.4.1 在 $\mathbf{Z}[x]$ 中, 多项式 $f(x)=x^n+x^{n-1}+\cdots+x+1, g(x)=x-1$ 都是本原多项式, $h(x)=4x-2$ 不是本原多项式. 容易知道, 若多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 的系数中有等于 1 的, 则 $f(x)$ 是本原多项式, 如首 1 多项式一定是本原多项式.

例 3.4.2 在 $\mathbf{Z}_3[x]$ 中, 多项式 $f(x)=x^2+x+\overline{1}$ 是本原多项式. 由于 $g(x)=\overline{2}x-\overline{1}=\overline{2}(x-\overline{2})$, $\overline{2}$ 在 $\mathbf{Z}_3$ 中是可逆的, 故 $g(x)$ 也是本原多项式.

思考题 3.4.1 *若 p 为素数, $\mathbf{Z}_p[x]$ 的多项式都是本原多项式吗?*

是的. 这是由于对任意的多项式 $f(x)\in\mathbf{Z}_p[x]$, 若 a 是 $f(x)$ 的系数的公因子, 则 a 是乘法可逆元, 因此 $f(x)$ 是本原多项式.

思考题 3.4.2 *设 R 是唯一因子分解环, 不可约多项式 $f(x)\in R[x]$ 一定是本原多项式吗? 反过来呢?*

容易看出, 次数大于等于 1 的不可约多项式 $f(x)\in R[x]$ 一定是本原多项式. 反过来, 如在 $\mathbf{Z}[x]$ 中, 多项式 $f(x)=x^2+4x+3$ 是本原多项式, 但 $f(x)=x^2+4x+3=(x+3)(x+1)$, 所以本原多项式 $f(x)\in R[x]$ 不一定是不可约多项式.

2 Gauss 引理

定理 3.4.1(Gauss 引理) *设 R 是唯一因子分解环, 则两个本原多项式 $f(x)$, $g(x)\in R[x]$ 的乘积 $f(x)g(x)$ 仍然是本原多项式.*

证明 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$$

都是本原多项式. 将 $f(x)g(x)$ 展开成

$$f(x)g(x)=c_{n+m}x^{n+m}+c_{n+m-1}x^{n+m-1}+\cdots+c_1x+c_0,$$

则

$$c_k=\sum_{i+j=k}a_ib_j.$$

反证法. 假如 $f(x)g(x)$ 不是本原多项式, 则存在 R 中的不可逆元 p 整除每个 c_i. 设 a_r 是 $f(x)$ 中从左边数起第一个不被 p 整除的系数. 设 b_s 是 $g(x)$ 中从左边

数起第一个不被 p 整除的系数. 则

$$c_{r+s} = a_r b_s + \sum_{i>0} a_{r-i} b_{s+i} + \sum_{i>0} a_{r+i} b_{s-i},$$

它不被 p 整除, 矛盾. 由反证法原理可知, $f(x)g(x)$ 是本原多项式. ■

思考题 3.4.3　*设 R 是唯一因子分解环, 若两个多项式 $f(x), g(x) \in R[x]$ 的乘积 $f(x)g(x)$ 是本原多项式, 则 $f(x)$ 和 $g(x)$ 都是本原多项式吗?*

是的. 实际上, 设 $f(x) = af_1(x)$, $g(x) = bg_1(x)$, 这里 $a, b \in R$, $f_1(x)$ 和 $g_1(x)$ 都是本原多项式, 则由上面的 Gauss 引理可知, $f_1(x)g_1(x)$ 为本原多项式. 由于 $f(x)g(x)$ 是本原多项式, 故 ab 是乘法可逆元, 因此由 $a(b(ab)^{-1}) = e$ 可知 a 是乘法可逆元. 由 $((ab)^{-1}a)b = e$ 可知 b 是乘法可逆元, 所以 $f(x) = af_1(x)$ 和 $g(x) = bg_1(x)$ 分别都是本原多项式.

3　分式域中的本原多项式

由于 $\mathbf{Q}[x]$ 一个本原多项式能否分解成两个次数较低的有理系数多项式的乘积与它能否分解成两个次数较低的整数系数多项式的乘积是一致的, 故在唯一因子分解环 R 和它的分式域 F 中, 一样可以考虑一个本原多项式在 $F[x]$ 中分解成两个次数较低的 $F[x]$ 的多项式的乘积, 与它可分解成两个次数较低的 $R[x]$ 中的多项式的乘积是否一致的问题.

引理 3.4.1　*设 R 是唯一因子分解环, F 为 R 的分式域, $f(x), g(x)$ 都是本原多项式, 若本原多项式 $f(x), g(x) \in R[x]$ 在 $F[x]$ 中相伴, 则它们在 $R[x]$ 中也是相伴的.*

证明　由于本原多项式 $f(x), g(x) \in R[x]$ 在 $F[x]$ 中相伴, 故存在 $c \in F$, 使得

$$f(x) = cg(x).$$

由 $c \in F$ 可知, 有 $a, b \in R$, 使得 $c = \dfrac{a}{b} \in F$, 并且 $\gcd(a, b) = 1$. 于是

$$bf(x) = ag(x).$$

设 $f(x)$ 和 $g(x)$ 的第 i 次项系数分别为 c_i 和 d_i, 比较上式两边第 i 次项的系数得 $bc_i = ad_i$. 假如 b 不是乘法可逆元, 由于 b 与 a 互素, 上面等式推出 b 整除 d_i, 从而 b 整除 $g(x)$ 的每个系数, 但这与 $g(x)$ 是本原多项式相矛盾. 所以 b 是乘法可逆元. 同理可证 a 也是乘法可逆元. ■

定理 3.4.2 *设 R 是唯一因子分解环, F 为 R 的分式域, 若 $R[x]$ 的一个本原多项式在 $F[x]$ 中可约, 则它可分解成两个次数较低的 $R[x]$ 中的多项式的乘积.*

证明 设 $f(x)$ 是 $R[x]$ 的一个本原多项式, $f(x)$ 在 $F[x]$ 中可约, 则存在 $g(x), h(x) \in F[x]$, 满足 $\deg(g) < \deg(f), \deg(h) < \deg(f)$, 使得 $f(x) = g(x)h(x)$. 故一定有 $r, s \in F$, 使 $rg(x), sh(x)$ 为 $R[x]$ 的本原多项式.

根据 Gauss 引理, 等式

$$rsf(x) = [rg(x)][sh(x)]$$

的左边是一个本原多项式.

由引理 3.4.1 得知, 本原多项式 $rsf(x) \in R[x]$ 和 $[rg(x)][sh(x)] \in R[x]$ 在 $F[x]$ 中相伴时, 它们在 $R[x]$ 中也是相伴的, 因此 rs 是 R 中的乘法可逆元, 所以 $f(x)$ 可分解成两个次数较低的 $R[x]$ 中的多项式的乘积. ■

3.5 唯一因子分解环上的多项式

对于整系数多项式 $f(x) \in \mathbf{Z}[x]$, $f(x)$ 在有理数域 $\mathbf{Q}$ 上可约的充分与必要条件是 $f(x)$ 在整数环 $\mathbf{Z}$ 上可约.

引理 3.5.1 *设 R 是一个唯一因子分解环, F 是它的分式域.*

(1) $R[x]$ 中的乘法可逆元是 R 中的乘法可逆元.

(2) 次数大于零的 $f(x) \in R[x]$ 是 $R[x]$ 中的不可约元当且仅当 $f(x)$ 是本原多项式并且它在 $F[x]$ 中不可约.

证明 (1) 设 $g(x)$ 是 $R[x]$ 中的一个乘法可逆元. 则存在 $h(x) \in R[x]$ 使 $g(x)h(x) = 1$, 因此 $\deg(g) = \deg(h) = 0$, 即 $g(x)$ 和 $h(x)$ 都是 R 中的非零元素, 所以 $g(x)$ 是 R 中的乘法可逆元.

(2) 先设 $f(x)$ 是 $R[x]$ 中的不可约元. 令 a 为 $f(x)$ 的系数的最大公因子, 则 $f(x) = af_1(x)$, 其中 $f_1(x)$ 是本原多项式. 由于 $\deg(f_1) = \deg(f) > 0$, 故 $f_1(x)$ 不是乘法可逆元, 因此 a 是乘法可逆元, 所以 $f(x)$ 是本原多项式.

若 $f(x)$ 在 $F[x]$ 中可约, 则它可分解成两个次数较低的 $R[x]$ 中的多项式的乘积, 但这将与 $f(x)$ 的不可约性矛盾, 所以 $f(x)$ 在 $F[x]$ 中不可约.

反之, 设 $R[x]$ 中的本原多项式 $f(x)$ 在 $F[x]$ 中不可约. 假定存在 $g(x), h(x) \in R[x]$, 使得 $f(x) = g(x)h(x)$. 由于 $f(x)$ 在 $F[x]$ 中不可约, 故 $\deg(g) = 0$ 或 $\deg(h) = 0$, 不妨设 $\deg(g) = 0$, 于是 $g(x)$ 是 R 中的非零元素 c. 由于 $f(x)$ 是本原多项式, c 是乘法可逆元, 所以 $f(x)$ 是 $R[x]$ 中的不可约元. ■

有了以上的准备, 就可以证明下面定理了.

定理 3.5.1　*设 R 是唯一因子分解环, 则 $R[x]$ 也是唯一因子分解环.*

证明　(1) 设 $f(x) \in R[x]$ 不等于零, 对 $\deg(f)$ 用归纳法来证明 $f(x)$ 可以分解成一个乘法可逆元和若干个不可约元的乘积.

若 $\deg(f)$=0, 则 $f \in R$ 由于 R 是唯一因子分解环, $f(x)$ 可以分解成一个乘法可逆元和若干个不可约元的乘积.

假设 $\deg(f) < n$ 时, $f(x)$ 可以分解成一个乘法可逆元和若干个不可逆元的乘积.

若 $\deg(f) = n$, 则 $f = cf_1$, 其中 $c \in R, f_1$ 是一个本原多项式. 将 c 分解成 $c = dc_1c_2\cdots c_r$, 其中 d 是乘法可逆元, $c_1, c_2, \cdots, c_r$ 是不可约元.

如果 f_1 不可约, 则 $f = dc_1c_2\cdots c_rf_1$ 已经是需要的分解式.

如果 f_1 可约, 则根据定理 3.3.2, 存在 $g(x), h(x) \in R[x]$, 使得 $f(x) = g(x)h(x)$, 其中 $\deg(g) < \deg(f) = n$, $\deg(h) < \deg(f) = n$. 根据归纳假设, $g(x)$ 和 $h(x)$ 都能作不可约分解, 于是 $f(x)$ 也可以作不可约分解.

(2) 设 $cp_1(x)\cdots p_s(x) = dq_1(x)\cdots q_t(x)$, 其中 c, d 是乘法可逆元, $p_1(x), \cdots, p_s(x), q_1(x), \cdots, q_t(x)$ 都是 $R[x]$ 中的不可约元. 不妨设

$$p_1(x), \cdots, p_u(x), q_1(x), \cdots, q_v(x) \in R,$$

$$p_{u+1}(x), \cdots, p_s(x), q_{v+1}(x), \cdots, q_t(x) \notin R.$$

设根据引理 3.5.1 的 (2), $p_{u+1}(x), \cdots, p_s(x), q_{v+1}(x), \cdots, q_t(x)$ 都是本原多项式并且它们在 $F[x]$ 中也不可约. 再根据 Gauss 引理, 乘积 $p_{u+1}(x)\cdots p_s(x)$ 和 $q_{v+1}(x)\cdots q_t(x)$ 都是本原多项式. 于是

$$p_1(x)\cdots p_u(x) = \lambda q_1(x)\cdots q_v(x),$$

$$p_{u+1}(x)\cdots p_s(x) = \mu q_{v+1}(x)\cdots q_t(x),$$

其中 λ, μ 是乘法可逆元. 由于 $p_1(x), \cdots, p_u(x), q_1(x), \cdots, q_v(x) \in R$, 故不妨记为 $p_1, \cdots, p_u, q_1, \cdots, q_v$, 因 R 是唯一因子分解环, 故 $u = v$, 且经适当的重新排列后, p_i 和 q_i 相伴, 这里 $1 \leqslant i \leqslant u$.

根据定理 3.3.2 有 $s = t$, 并经适当的重新排列后, p_i 和 q_i 在 $F[x]$ 中相伴, 这里 $u \leqslant i \leqslant s$. 由引理 3.4.1 可知, p_i 和 q_i 在 $R[x]$ 中也相伴. ■

由上面定理和数学归纳法, 可以证明下面推论成立.

推论 3.5.1 设 R 是一个唯一因子分解环, 则 $R[x_1, x_2, \cdots, x_n]$ 是唯一因子分解环.

推论 3.5.2 (1) 对任何域 F, 多项式环 $F[x_1, x_2, \cdots, x_n]$ 是唯一因子分解环.

(2) $\mathbf{Z}[x_1, x_2, \cdots, x_n]$ 是唯一因子分解环.

不过, 一般来说, 要将域 F 上的多项式分解成不可约多项式的乘积是不容易的, Zierler 和 Brillhart 在 1968 年和 1969 年讨论了 $\mathbf{Z}_2$ 上的多项式的分解, 给出了形如 $x^n + x^k + 1 (0 < k < n)$ 的多项式在 $2 \leqslant n \leqslant 1000$ 的不可约分解①②.

3.6 非交换环上的多项式

非交换可除环上的多项式具有很多奇特的性质.

定义 3.6.1 设 R 是一个非交换可除环, 表达式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

称为 R 上的一个多项式, 这里 $a_n, a_{n-1}, \cdots, a_1, a_0 \in R$, x 与 R 中的所有元都可交换, 并且 $1x = x$. R 上的一个多项式全体记为 $R[x]$.

定义 3.6.2 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, 对于 $a \in R$, 定义

$$f(a) = a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0,$$

① Zierler N, Brillhart J. On primitive trinomials (mod 2). Information and Control, 1968, 13: 541–554.

② Zierler N, Brillhart J. On primitive trinomials (mod 2). II. Information and Control, 1969, 14: 566–569.

称 $f(a)$ 为 $f(x)$ 在 a 处的值. 如果 $f(a)=0$, 则称 a 为 $f(x)$ 在非交换可除环 R 的一个根 (或零点).

容易知道, 虽然 $\sum\limits_{i=0}^{n} a_i x^i = \sum\limits_{i=0}^{n} x^i a_i$, 但是对于 $a \in R$, 有可能 $\sum\limits_{i=0}^{n} a_i a^i = \sum\limits_{i=0}^{n} a^i a_i$ 不成立. 还要注意 $f(x)=a_2x^2+xa_1+a_0$ 不是多项式, 多项式的项中的系数一定要在 x 的左边.

思考题 3.6.1　若 $f(x)=g(x)h(x)$, 则对于 $a \in R$, $f(a)=g(a)h(a)$ 是否一定成立?

不一定.

例 3.6.1　设 R 是非交换环, $a,b \in R, ab \neq ba$, 则对于 $g(x)=x-a$, $h(x)=x-b$, 有 $f(x)=g(x)h(x)=x^2-(a+b)x+ab$, 故

$$f(a)=a^2-(a+b)a+ab=ab-ba \neq 0,$$

但 $g(a)h(a)=0$. 因此 $f(a)=g(a)h(a)$ 不成立.

实际上, 在所有整数上的 2×2 矩阵全体构成的非交换环 $M_2(\mathbf{Z})$ 中, 只需取

$$a=\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad b=\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

则容易知道, 对于环 $M_2(\mathbf{Z})$ 上的多项式 $g(x)=x+a$, $h(x)=x-a$, 有

$$f(x)=g(x)h(x)=x^2-a^2.$$

但 $f(b)=b^2-a^2=0$, 而

$$\begin{aligned} g(b)h(b) &= \left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}+\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\right)\left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}-\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\right) \\ &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}=\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \end{aligned}$$

所以, $f(b) \neq g(b)h(b)$.

定义 3.6.3　设 $a \in R$, $f(x) \in R[x]$, 若 $f(a)=0$, 则称 a 为 $f(x)$ 的**右根**.

一般都只讨论右根, 因此就将右根简称为**根**.

不难建立非交换环上剩余定理.

定理 3.6.1 设 R 是非交换环, $a \in R$ 是非零多项式 $f(x) \in R[x]$ 的根的充要条件为 $x-a$ 是 $f(x)$ 在 $R[x]$ 的右除因子. $R[x]$ 有根 a 的多项式全体为左理想 $R[x](x-a)$.

证明 若 $x-a$ 是 $f(x)$ 在 $R[x]$ 的右除因子, 则 $f(x)$ 具有形式:

$$\left(\sum_{i=0}^{n} c_i x^i\right)(x-a) = \sum_{i=0}^{n} c_i x^{i+1} - \sum_{i=0}^{n} c_i a x^i,$$

故

$$f(a) = \sum_{i=0}^{n} c_i a^{i+1} - \sum_{i=0}^{n} c_i a \cdot a^i = 0.$$

反过来, 若 $f(a)=0$, 则由于有某个 $g(x) \in R[x]$ 和 $b \in R$, 使得

$$f(x) = g(x)(x-a) + b.$$

由于 $x-a$ 是 $g(x)(x-a)$ 在 $R[x]$ 的右除因子, 故 a 是 $g(x)(x-a)$ 的根, 因而 $0 = f(a) = b$, 所以 $x-a$ 是 $f(x)$ 在 $R[x]$ 的右除因子. ■

性质 3.6.1 设 R 是可除环, $f(x) = g(x)h(x) \in R[x]$, 若 $a \in R$, 使得 $b = h(a) \neq 0$, 则

$$f(a) = g(bab^{-1})h(a).$$

证明 设 $g(x) = \sum_{i=0}^{n} b_i x^i$, 则 $f(x) = \sum_{i=0}^{n} b_i h(x) x^i$, 故

$$\begin{aligned} f(a) &= \sum_{i=0}^{n} b_i h(a) a^i \\ &= \sum_{i=0}^{n} b_i b a^i = \sum_{i=0}^{n} b_i b a^i b^{-1} b \\ &= \sum_{i=0}^{n} b_i (bab^{-1})^i b \\ &= g(bab^{-1})h(a). \end{aligned}$$

■

推论 3.6.1 设 R 是可除环, $f(x) = g(x)h(x) \in R[x]$, 若 $a \in R$ 是 f 的根, 并且 a 不是 h 的根, 则 bab^{-1} 是 g 的根, 这里 $b = h(a)$.

定理 3.6.2　设 R 是可除环, $f(x) \in R[x]$, 并且多项式 $f(x)$ 的系数都在 R 的中心中, $C(R) = \{a \in R | ab = ba$ 对任意 $b \in R\}$ 成立, 若 $a \in R$ 是 f 的根, 并且 $b \neq 0$, b 可逆, 则 bab^{-1} 是 f 的根.

证明　对于 $f(x) = \sum_{i=0}^{n} a_i x^i$, 若 $a \in R$ 是 f 的根, 并且 $b \neq 0$, 则

$$f(bab^{-1}) = \sum_{i=0}^{n} a_i (bab^{-1})^i = \sum_{i=0}^{n} a_i (ba^i b^{-1}).$$

由于 $a_i \in C(R)$, 故 $\sum_{i=0}^{n} a_i (ba^i b^{-1}) = b \left(\sum_{i=0}^{n} a_i a^i \right) b^{-1} = 0$, 所以 bab^{-1} 是 f 的根. ■

例 3.6.2　对于实数域上四元数除环 H, 由于多项式 $f(x) = x^2 + 1$ 的系数都在 H 的中心中, 因此当 $a \in H$ 是 f 的根, 并且 b 可逆时, 则 bab^{-1} 一定是 f 的根.

域 R 上的 n 次多项式最多只有 n 个根, 对于非交换环情形, 可以考虑同样的问题, 去掉交换条件之后, 多项式的根会变得很有趣.

思考题 3.6.2　非交换环 R 上的 n 次多项式最多只有 n 个根吗?

不一定, 对于实数域上四元数除环 H, i, j, k 显然都满足方程 $x^2 + 1 = 0$, 因此 2 次方程 $x^2 + 1 = 0$ 已经有 3 个根. 实际上, 任何 i 的共轭元都是方程的根, 故对任何可逆元 $a \in R$, 都有 $(aia^{-1})^2 + 1 = 0$, 所以方程 $x^2 + 1 = 0$ 有无穷多个根.

定理 3.6.3(Gordon-Motzkin定理)　设 R 是可除环, $f(x) \in R[x]$, 若 $f(x)$ 是 n 次多项式, 则 f 的根在 R 的最多 n 个共轭类中. 如果存在不同的 $a_i \in R$, 使得 $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$, 那么 f 的任何根 a 一定与某个 a_i 共轭.

证明　对 n 用归纳法来证明.

(1) 若 $n = 1$, 则容易知道结论成立.

(2) 假设结论对于 $n - 1$ 次多项式都成立.

(3) 对于 n 次多项式 $f(x)$, c 是 f 的一个根, 则存在 $g(x) \in R[x]$, 使得 $f(x) = g(x)(x - c)$, 假如 $d \neq c$ 是 f 的另外一个根, 则由推论 3.6.1 可知 d 与 $g(x)$ 的某个根共轭. 根据假设结论对于 $n - 1$ 次多项式都成立, 即 g 的根在 R 的最多 $n - 1$ 个共轭类中, 所以 f 的根在 R 的最多 n 个共轭类中. ■

若 R 是交换环, 则每个共轭类只有一个元素, 因此交换环 R 上的 n 次多项式 $f(x)$ 在 R 最多只有 n 个根.

思考题 3.6.3 *若 a 是非交换环 R 上的多项式 $f(x)$ 的根, b 与 a 共轭, 则 b 也是 $f(x)$ 的根吗?*

不一定.

例 3.6.3 实数域上四元数除环 H, 它是非交换环, 对于多项式 $f(x)=(x-i)(x-j)$, 容易知道 $(x-i)(x-j)=x^2-ix-jx+ij=0$, 故 $j^2-ij-jj+ij=0$, 因此 j 是它的一个根. 但由于 $(-j)^2-i(-j)-j(-j)+ij\neq 0$, 因而 $-j$ 不是方程 $(x-i)(x-j)=0$ 的一个根. 容易知道 $-j=i\cdot j\cdot i^{-1}$, 故 $-j$ 与 j 共轭, 但 $-j$ 不是它的一个根.

定理 3.6.4 *设 R 是环, $f(x)=g(x)h(x)\in R[x]$, 若 $a\in R$ 是 h 的根, 则 a 是 f 的根.*

证明 设 $g(x)=\sum\limits_{i=0}^{n}b_ix^i$, 则 $f(x)=g(x)h(x)=\left(\sum\limits_{i=0}^{n}b_ix^i\right)h(x)=\sum\limits_{i=0}^{n}b_ih(x)x^i$, 故 $f(a)=\sum\limits_{i=0}^{n}b_ih(a)a^i=0$, 所以 a 是 f 的根. ■

思考题 3.6.4 *设 R 是环, $f(x)=g(x)h(x)\in R[x]$, 若 $a\in R$ 是 g 的根, 则 a 是 f 的根吗?*

不一定. 实际上, 在所有实数上的 2×2 矩阵全体构成的非交换环 $M_2(R)$ 中, 只需取

$$a=\begin{bmatrix}1&0\\0&0\end{bmatrix},\quad b=\begin{bmatrix}0&1\\0&0\end{bmatrix},\quad c=\begin{bmatrix}0&0\\1&0\end{bmatrix}.$$

设 $g(x)=bx, h(x)=c$, 则 $g(a)=ba=0$, 因此 a 是 g 的根, 但

$$f(a)=bca=a\neq 0,$$

所以, a 不是 f 的根. ■

环上的多项式还可以用来研究环本身的性质, 1997 年 Rege 和 Chhawchharia 引入了 Armendariz 环①.

① Rege M B. Chhawchharia S. Armendariz rings. Proc. Japan Acad. Ser. A Math. Sci., 1997, 73(1): 14–17.

定义 3.6.4　设 R 是环, 若多项式 $f(x)=\sum\limits_{i=0}^{m}a_ix^i$, $g(x)=\sum\limits_{i=0}^{n}b_ix^i\in R[x]$ 满足 $f(x)g(x)=0$ 时, 一定有 $a_ib_j=0$ 对任意的 i 和 j 都成立, 则称环 R 为 Armendariz 环.

将它称为 Armendariz 环是由于 Armendariz 在 1974 年注意到了具有这种性质的环①.

例 3.6.4　对于任意的正整数 n, $\mathbf{Z}/n\mathbf{Z}$ 是 Armendariz 环.

容易知道 Armendariz 环的子环还是 Armendariz 环, 但 Armendariz 环的商环就不一定是 Armendariz 环.

近年来, 人们对 Armendariz 环进行了系统的研究, 并给出了多种形式的推广②③.

习　题　三

3.1　设 $\mathbf{R}[x]$ 为实数 $\mathbf{R}$ 上的多项式环, 理想 $I=(x), J=(x+1)$, 试求 $I\cap J$ 和 $I+J$.

3.2　在 $\mathbf{Z}_3[x]$, 设 $f(x)=\overline{2}x^4+\overline{2}x+\overline{1}, g(x)=x^2+x+\overline{2}$, 试求出 $g(x)$ 除 $f(x)$ 的商和余式.

3.3　试证明有理数域 $\mathbf{Q}$ 上的多项式 $f(x)$ 和 $g(x)$ 相等的充要条件为对任意的 $a\in\mathbf{Q}$, 有 $f(a)=g(a)$.

3.4　设 F 为域, $a_1,a_2,\cdots,a_n$ 为 F 中 n 个不同的元素, 试证明存在域 F 上的多项式 $f(x)$, 使得对 $a_i\in F$, 有 $f(a_i)=1$ 对任意 i 成立.

3.5　试证明 $\mathbf{Z}[x]$ 不是主理想交换整环.

3.6　试给出例子说明环 $R[x]$ 中的 m 次与 n 次多项式的乘积可能不是一个 $m+n$ 次多项式.

3.7　试求出 $\mathbf{Z}_5$ 上多项式 $f(x)=\overline{4}x^3-\overline{2}x^2+x+\overline{3}$ 的所有根.

① Armendariz E P. Anote on extensions of Baer and P.P.-rings. J. Austral. Math. Soc., 1974, 18: 470–473.

② Agayev N. Harmanci A. Halicioglu S. Extended Armendariz rings. Algebras Groups Geom., 2009, 26(4): 343–354.

③ Antoine R. Examples of Armendariz rings. Comm. Algebra. 2010, 38(11): 4130–4143.

3.8 试求出 $\mathbf{Z}_3$ 上的所有 2 次不可约多项式.

3.9 $2x+2$ 在 $\mathbf{Z}[x]$ 和 $\mathbf{Q}[x]$ 中是不可约元吗?

3.10 试将 x^9-1 在 $\mathbf{Z}[x]$ 中作素因子分解.

3.11 设 R 是整环, $a,b\in R$, 试证明理想 (a) 与理想 (b) 相等的充要条件为 a 与 b 相伴.

3.12 试证明 $f(x)=x^2+1\in\mathbf{Z}[x]$ 是整数上的多项式环 $\mathbf{Z}[x]$ 上的不可约元.

3.13 设 R 是主理想交换环, 若 $a_1,a_2,\cdots,a_n\in R$, 试证明 $a_1,a_2,\cdots,a_n$ 互素的充要条件为存在 $b_1,b_2,\cdots,b_n\in R$, 使得 $a_1b_1+a_2b_2+\cdots+a_nb_n=1$.

3.14 设 R 是主理想交换整环, 试证明对于任意 $a,b\in R$, a,b 都有最大公约元 d 存在, 并且有 $u,v\in R$, 使得 $d=ua+vb$.

3.15 设 R 为唯一分解交换整环, 若 R 只有有限个乘法可逆元, 试证明对任意非零元 $a\in R$, a 只能有有限个因子.

3.16 设 R 是有理数域上的 2×2 阶矩阵构成的非交换环, 若 $f(x),g(x)\in R$,

$$f(x)=\begin{bmatrix}2&1\\0&0\end{bmatrix}x^2+\begin{bmatrix}0&0\\1&0\end{bmatrix}x+\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad g(x)=\begin{bmatrix}0&1\\-1&0\end{bmatrix}x+\begin{bmatrix}1&1\\1&1\end{bmatrix}.$$

试分别求出 $f(x)$ 被 $g(x)$ 右除所得到的右余式, 以及被 $g(x)$ 左除所得到的左余式.

~~~~~~

伯恩赛德 (W.Burnside)1852 年 7 月 2 日生于英国伦敦, 1871 年入剑桥圣约翰学院学习, 1873 年转入彭布罗克学院. 1875-1886 年任研究员, 1885 年起任格林尼治皇家海军学院数学教授. 1893 年选为英国皇家学会会员, 1906-1908 年任伦敦数学会会长. 前期主要研究应用数学, 还研究椭圆函数以及微分几何等. 1892 年起研究群论, 是群表示论的主要创始人之一, 并应用群表示论证明了 p^mq^n 阶群是可解群 (p, q 为素数). 1899 年获伦敦数学会德 · 摩根奖. 他所著的 *Theory of Groups of Finite Order* (Cambridge University Press, 1897) 是有限群论的第一部系统著作, 对群论的发展有着非常深刻的影响. 1900 年左右, 伯恩赛德提出了一个著名的猜想: 一个奇数阶群 G 必存在一个正规子群列: $\{e\}=G_0\lhd G_1\lhd\cdots\lhd G_n=G$, 使得每个 $G_{i+1}/G_i(0\leqslant i\leqslant n-1)$ 是交换群. 这一猜想对有限单群分类问题的研究起了重大作用. 50 多年后, 猜想被费特 (Feit) 和汤普森 (Thompson) 在一篇长达 255 页
~~~~~~

的论文中所证明. 他的另一重要猜想是关于群 $B(m,n)$ 的. 1994 年, 柴尔曼诺夫 (Zelmanov) 由于在这一猜想方面的工作而获得菲尔兹奖.

学习指导

本章重点

1. 域 F 上的多项式环 $F[x]$ 的任何理想都是主理想.

2. 任意域上 F 的单变量多项式环 $F[x]$ 是唯一因子分解环.

3. 设 R 是唯一因子分解环, 则 $R[x]$ 也是唯一因子分解环.

基本要求

1. 多项式部分.

(1) 复习高等代数中数域上的多项式性质, 熟练掌握交换环上多项式的基本运算性质.

(2) 熟练掌握交换环上多项式的带余除法.

(3) 熟练掌握交换环上多项式根的相关性质.

(4) 主理想整环定义和例子: 整数环和域上多项式环都是主理想整环, 但整环上的多项式环不一定是主理想整环.

(5) 一个交换整环 R 上的多变量多项式 $R[x_1,x_2,\cdots,x_n]$ 是一个交换整环.

2. 唯一分解整环的性质.

(1) 在一般的交换环中, 素元一定是不可约元, 但不可约元不一定是素元.

(2) 在唯一分解整环中, 不可约元和素元二者是一样的.

(3) 在唯一分解整环中, 若 $a|bc,(a,b)=1$, 则 $a|c$.

释疑解难

1. 整环不一定是唯一分解整环. 如在整环 $\mathbf{Z}[\sqrt{3}\mathrm{i}] = \{a + b\sqrt{3}\mathrm{i} | a, b \in \mathbf{Z}\}$ 中, $4 = 2 \cdot 2 = (1 + \sqrt{3}\mathrm{i})(1 - \sqrt{3}\mathrm{i})$.

2. 判断一个整环是不是一个唯一分解整环有时是比较难的.

3. 域是唯一分解整环, 这是由于域只有零元和可逆元, 任意 $a \in F$, $a = a \cdot 1$, a 可逆, 1 是不可约元, 故在唯一分解整环讨论中域并无多大的实际意义.

4. $\mathbf{Z}[x]$ 是唯一分解整环, 但不是主理想整环, 例如 $\mathbf{Z}[x]$ 的理想 $(2, x)$ 不是主理想.

5. 主理想整环是唯一分解整环.

6. 在除法算式的定理中, R 是一个交换环, $f(x), g(x) \in R[x]$, $g(x) \neq 0$, 如果不要求 $g(x)$ 的首项系数是 R 中的乘法可逆元, 定理成立吗?

不一定. 在整数多项式环 $\mathbf{Z}[x]$, 对于 $f(x) = x^2 + 1$, $g(x) = 2x$, $g(x)$ 的首项系数不是 $\mathbf{Z}$ 中的乘法可逆元, 不存在 $q(x) \in \mathbf{Z}[x]$, 使得 $f(x) = q(x)g(x) + r(x)$.

7. 多项式 $f(x)$ 是否可约依赖于它所在的多项式环, 如 $f(x) = x^2 - 3$ 在整数多项式环 $\mathbf{Z}[x]$ 中是不可约的, 但在实数多项式环 $\mathbf{R}[x]$ 中是可约的 $f(x) = x^2 - 3 = (x + \sqrt{3})(x - \sqrt{3})$.

8. 非交换可除环上的多项式是本章的难点, 主要是要理解非交换可除环上的多项式的定义, 要明白只有形如 $\sum_{i=0}^{n} a_i x^i$ 的才是多项式, 如 $f(x) = a_2 x^2 + x a_1 + a_0$ 不是多项式. 非交换环上的多项式具有很多与交换环上的多项式完全不同的性质.

9. 对于非交换可除环 R 上的多项式 $f(x), g(x) \in R[x]$, 可能存在不同的 $q_1(x)$, $q_2(x) \in R[x]$ 和 $r_1(x), r_2(x) \in R[x]$, 使得

$$f(x) = q_1(x)g(x) + r_1(x), \quad \text{并且 } f(x) = g(x)q_2(x) + r_2(x).$$

整数环与整数环上的多项式的比较

整数环与整数环上的多项式有很多类似的性质, 每个整数都可以写成与多项式形式类似的式子, 如整数 $19641011 = 1 + 10 + 10^3 + 4 \cdot 10^4 + 6 \cdot 10^5 + 9 \cdot 10^6 + 10^7$, 实际上, 对于多项式 $f(x) = 1 + x + x^3 + 4x^4 + 6x^5 + 9x^6 + x^7$, 有 $19641011 = f(10)$. 它们是交换环论的基础, 因此要熟悉它们的性质.

整数环 $\mathbf{Z}$	整数环 $\mathbf{Z}$ 上的多项式 $\mathbf{Z}[x]$
$\mathbf{Z}$ 的分式域为有理数全体	分式域为有理多项式
$\left\{\frac{n}{m}\mid m,n\in\mathbf{Z},n\neq 0\right\}$	$\left\{\frac{f(x)}{g(x)}\mid f(x),g(x)\in\mathbf{Z}[x],g(x)\neq 0\right\}$
整环	整环
唯一分解环	唯一分解环
主理想交换整环	$\mathbf{Z}[x]$ 不是主理想交换整环, 如 2 和 x 生成的理想 $(2,\ x)$ 不是 $\mathbf{Z}[x]$ 的主理想.
素元 (素数) 一定是不可约元	素元一定是不可约元

解题技巧

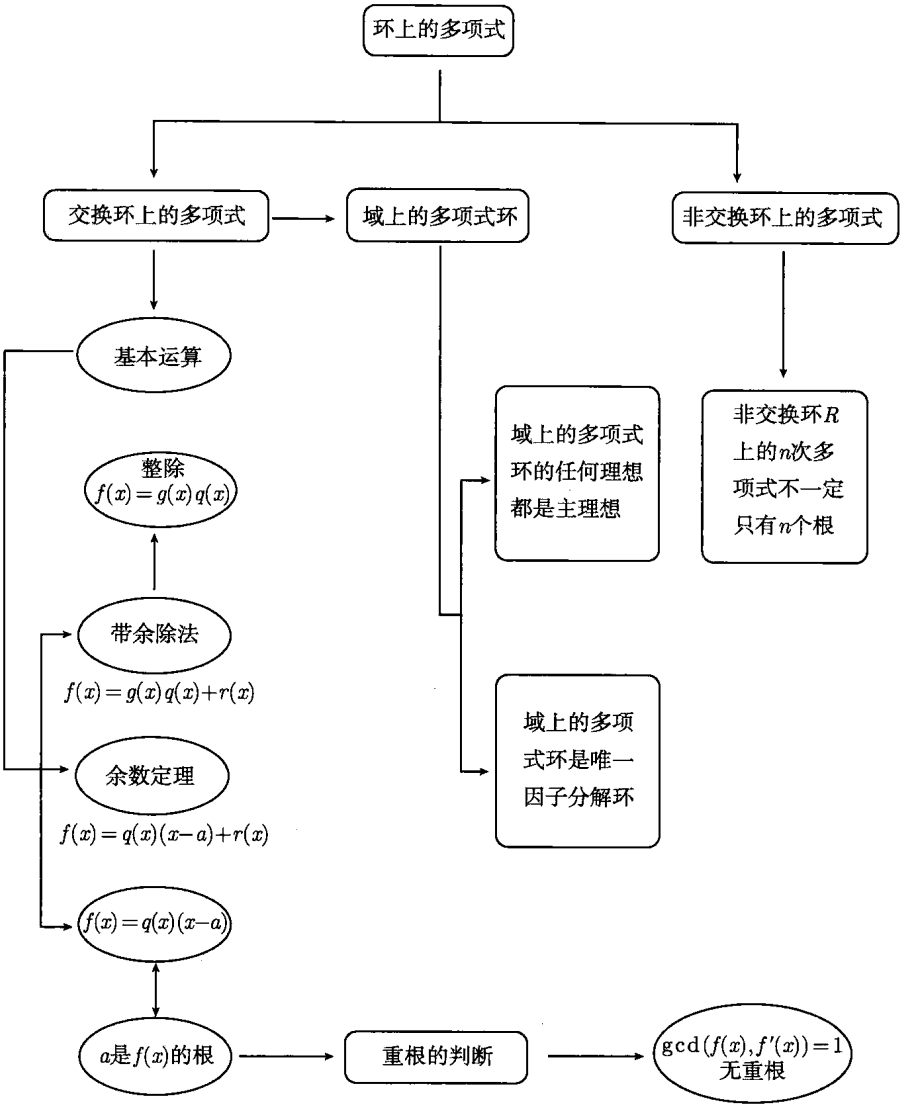
1. 对于环 R 上的多项式 $f(x),g(x)\in R[x]$, 求出 $q(x),r(x)\in R[x]$, 使得

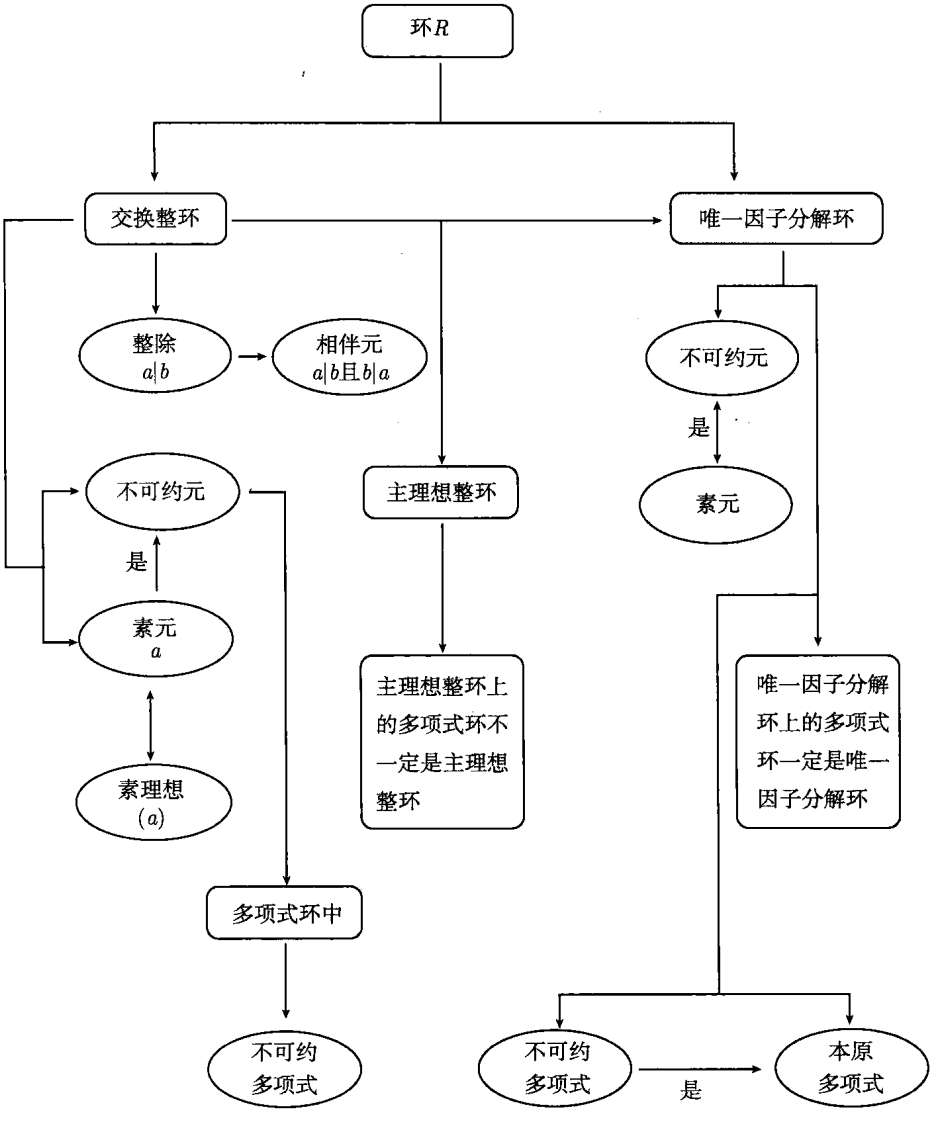
$$f(x)=q(x)g(x)+r(x).$$

2. 利用多项式 $f(x)$ 的根, 判断多项式 $f(x)$ 是否可约.

3. 将多项式 $f(x)$ 分解成不可约多项式的乘积.

知识点联系图


环上的多项式
交换环上的多项式
域上的多项式环
非交换环上的多项式
基本运算
整除
$f(x)=g(x)q(x)$
带余除法
$f(x)=g(x)q(x)+r(x)$
余数定理
$f(x)=q(x)(x-a)+r(x)$
$f(x)=q(x)(x-a)$
域上的多项式环的任何理想都是主理想
域上的多项式环是唯一因子分解环
非交换环R上的n次多项式不一定只有n个根
a是$f(x)$的根
重根的判断
$\gcd(f(x),f'(x))=1$
无重根


环R
交换整环
唯一因子分解环
整除
$a|b$
相伴元
$a|b$且$b|a$
不可约元
是
素元
不可约元
是
素元
a
素理想
(a)
主理想整环
主理想整环上的多项式环不一定是主理想整环
唯一因子分解环上的多项式环一定是唯一因子分解环
多项式环中
不可约多项式
不可约多项式
是
本原多项式

第4章 向量空间

数学中的一些美丽定理具有这样的特性：它们极易从事实中归纳出来，但证明却隐藏的极深.

Gauss (1777—1855, 德国数学家)

向量空间是 Peano 在 1888 年出版的书 *Geometrical Calculus* 中引进的. 在高等代数中, 向量空间都是在一个数域上来讨论. 有了域的概念, 就可以将向量空间的部分理论推广到域上的向量空间.


Giuseppe Peano (1858-1932)

4.1 向量空间

在解析几何中, 讨论过三维空间中的向量. 向量的基本属性是可以按平行四边形规律相加, 也可以与实数作数量乘法. 很多几何和力学对象的性质与向量的这两种运算有着密切的联系.

1 向量空间的定义

定义 4.1.1 设 F 是一个域, V 是一个 Abel 群 (用加法记它的群运算), 若有一个数乘运算

$$F \times V \to V,$$

$$(a, u) \mapsto au$$

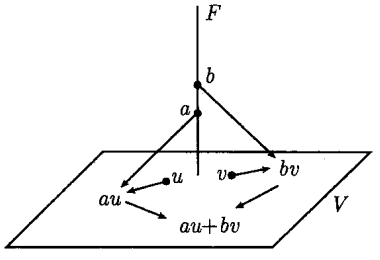
满足以下条件:

(1) $1u = u$ 对任意 $u \in V$ 成立;

(2) $(ab)u = a(bu)$ 对任意 $a, b \in F, u \in V$ 成立;

(3) $(a + b)u = au + bu$ 对任意 $a, b \in F, u \in V$ 成立;

(4) $a(u+w)=au+aw$ 对任意 $a\in F,u,w\in V$ 成立.



则称 V 为域 F 上的一个向量空间 (vector space) 或线性空间 (linear space), 向量空间中的元素称为向量 (vector), 域中的元素称为纯量 (scalar).

向量空间是一种比群和环复杂的代数结构, 它的数乘运算与环中的运算不一样, 向量空间的数乘运算是域 F 中的元素和 V 中的元素相乘.

例 4.1.1　设 F 是域, 则多项式环 $F[x]$ 为域 F 上的向量空间. 这里的加法就是多项式的相加, 数乘为若 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $c\in F$, 则

$$cf(x)=ca_nx^n+ca_{n-1}x^{n-1}+\cdots+ca_1x+ca_0.$$

例 4.1.2　设 $C[a,b]=\{u(t)|u(t)$ 为 $[a,b]$ 上的连续函数 $\}$, 则在函数相加和数乘下是实数域 $\mathbf{R}$ 上的向量空间. 不过要注意向量空间 $C[a,b]$ 的数乘运算与环 $C[a,b]$ 的乘法运算是完全不同的.

例 4.1.3　设 $p(x)$ 和 $q(x)$ 为 $(0,1)$ 上的连续函数, 微分方程

$$y''+p(x)y'+q(x)y=0$$

的所有解在函数相加和数乘下是实数域 $\mathbf{R}$ 上的向量空间.

思考题 4.1.1　含有非零元的最小向量空间含有多少个元素?

容易知道, $\mathbf{Z}_2=\{\overline{0},\overline{1}\}$ 是一个加法 Abel 群, 它可以看做域 $\mathbf{Z}_2$ 上的向量空间, 它只有两个元素.

2　向量空间的性质

容易知道, 向量空间有很多与数域上的向量空间一样的性质.

性质 4.1.1　设 V 是域 F 上的向量空间, 则对任意的 $a\in F$, $u\in V$, 有 $a0=0$, $0u=0$.

性质 4.1.2　设 V 是域 F 上的向量空间, 若对于 $a\in F$, $u\in V$, 有 $au=0$, 则一定有 $a=0$ 或 $u=0$.

证明 若 $au=0$, 但 $a\neq 0$, 则由于 F 是域, $a\in F$, 故存在 $a^{-1}\in F$, 使得 $a^{-1}au=a^{-1}0=0$, 所以 $u=0$. ■

由于域有两种运算, 故可以讨论它能否看做向量空间的问题.

定理 4.1.1 *设 V 是域, F 是 V 的子域, 则 V 是 F 上的向量空间.*

3 向量空间的子空间

向量空间 V 的一个对加法和数乘封闭的子集 W 称为 V 的一个子空间.

定义 4.1.2 *设 V 是一个向量空间, 若 W 为 V 的非空子集, 满足以下条件:*

(1) $0\in W$;

(2) $u+v\in W$ *对任意* $u,v\in W$ *成立*;

(3) $au\in W$ *对任意* $a\in F, u\in W$ *成立*.

则称 W 为 V 的一个子空间.

一般将向量空间 V 的零子空间和它本身称为 V 的平凡子空间, 从子空间的定义容易知道, F 是域时, 将 F 看做 F 上的向量空间, 则对于 F 的任意子空间 W, W 是域 F 的理想, 由于域只有平凡理想, 故下面结论成立.

定理 4.1.2 *设 F 是域, 将 F 看做 F 上的向量空间, 则 F 没有非平凡的子空间.*

例 4.1.4 域为 $\mathbf{Z}_{11}$ 的多项式全体 $\mathbf{Z}_{11}[x]$ 是一个向量空间, 令

$$W=\{a_3x^3+a_2x^2+a_1x+a_0|a_0,a_1,a_2,a_3\in\mathbf{Z}_{11}\},$$

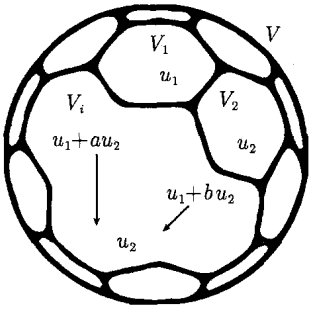
则 W 是 $\mathbf{Z}_{11}[x]$ 的一个子空间.

定理 4.1.3 *若 V 是无限域 F 上的向量空间, 则 V 不可能是有限个真子空间的并.*

证明 反证法. 假设 $V_1,V_2,\cdots,V_n$ 是满足 $V=V_1\cup V_2\cup\cdots\cup V_n$ 的真子空间中个数最少的真子空间.

取

$$u_1\in V_1,\quad u_1\notin V_2,\quad u_2\in V_2,\quad u_2\notin V_1\cup V_3\cup\cdots\cup V_n.$$



对于 $i=1,2,\cdots,n$, 令

$$F_i=\{a\in F|u_1+au_2\in V_i\}.$$

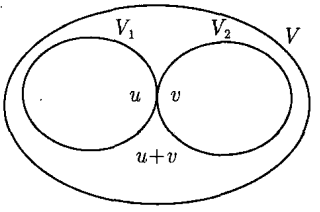
则 $F=F_1\cup F_2\cup\cdots\cup F_n$. 由于 F 是无限域, 故一定有某个 F_i 最少包含两个元素. 由于 $u_1\in V_1, u_1\notin V_2$, $u_2\in V_2$, 因此 $F_2=\varnothing$. 故存在某个 $i\neq 2$, 有两个不同的 $a,b\in F_i$, 使得 $u_1+au_2\in V_i$, 并且 $u_1+bu_2\in V_i$, 因而

$$(a-b)u_2=(u_1+au_2)-(u_1+bu_2)\in V_i,$$

故 $u_2\in V_i$. 但这与 $u_2\notin V_i$ 的选取相矛盾, 所以定理成立. ■

从上面的证明中可以看出, 下面结论成立.

定理 4.1.4　*若 V 是有限域 F 上的向量空间, V 是 n 个真子空间的并, 则一定有 $|F|<n$.*



例 4.1.5　设 V_1,V_2 是域 F 上的线性空间 V 的两个真子空间, 试证明 $V\neq V_1\cup V_2$.

证明　不妨设 V_1 和 V_2 没有相互包含的关系, 则存在 $u\in V_1, u\notin V_2, u\neq 0$, 并且存在 $v\in V_2, v\notin V_1$, $v\neq 0$. 此时一定有 $u+v\notin V_1$, 不然的话, 由 $u+v\in V_1$ 和 $u\in V_1$ 可知, $v\in V_1$, 与 $v\notin V_1$ 矛盾. 同理可知道 $u+v\notin V_2$, 因而 $u+v\in V$, 但 $u+v\notin V_1\cup V_2$, 所以 $V\neq V_1\cup V_2$.

4　线性无关和基

定义 4.1.3　*设 $u_1,u_2,\cdots,u_n\in V$ 是向量空间 V 的一组非零向量, 如果存在一组不全为零的纯量 $a_1,a_2,\cdots,a_n\in F$, 使得*

$$a_1u_1+a_2u_2+\cdots a_nu_n=0,$$

则称 $u_1,u_2,\cdots,u_n$ 线性相关, 否则称 $u_1,u_2,\cdots,u_n$ 线性无关.

定义 4.1.4　*设 S 是域 F 上的向量空间 V 中一个子集, 若*

$$W=\{a_1u_1+a_2u_2+\cdots+a_ku_k|a_1,a_2,\cdots,a_k\in F,u_1,u_2,\cdots,u_k\in S,$$
$$k \text{ 为某个正整数}\}$$

则称 W 是 S 张成的子空间, 记为 $W=<S>$.

例 4.1.6 设 F 是域, 则域 F 上的多项式空间 $F[x]$ 的子集 $\{1,x,x^2,\cdots,x^n\}$ 张成的子空间为所有次数小于等于 n 的多项式全体.

定义 4.1.5 一个张成整个向量空间 V 的线性无关集 S 称为 V 的一组基, 若 S 中的元素个数 n 有限, 则称 n 为向量空间 V 的维数, 记为 $\dim(V)$, 此时 V 称为有限维向量空间. 若 S 中的元素个数是无穷, 则称向量空间 V 是无穷维的.

例 4.1.7 $C[0,1]$ 是实数域 R 上的向量空间, $S=\{x^\alpha|\alpha\in[0,1]\}$ 是 $C[0,1]$ 的一个线性无关集, S 包含不可数个元素.

例 4.1.8 设 F 是域, 则域 F 上的多项式空间 $F[x]$ 有一组基 $\{1,x,x^2,\cdots,x^n,\cdots\}$.

例 4.1.9 设 V 是实数 $\mathbf{R}$ 上的所有函数构成的实数域 $\mathbf{R}$ 上的向量空间, 试证明 $\left\{\dfrac{1}{x-u}|u\in\mathbf{R}\right\}$ 是 V 的线性无关集.

证明 反证法. 假设存在互不相同的 $u_1,u_2,\cdots,u_n\in\mathbf{R}$, 使得 $\dfrac{1}{x-u_1}$, $\dfrac{1}{x-u_2},\cdots,\dfrac{1}{x-u_n}\in V$ 是线性相关的, 则存在不全为零的 $a_1,a_2,\cdots,a_n\in\mathbf{R}$, 使得

$$\frac{a_1}{x-u_1}+\frac{a_2}{x-u_2}+\cdots+\frac{a_n}{x-u_n}=0.$$

故

$$\sum_{i=1}^{n}(x-u_1)(x-u_2)\cdots(x-u_{i-1})a_i(x-u_{i+1})\cdots(x-u_n)=0.$$

令 $x=u_i$, 则 $a_i=0(i=1,2,\cdots,n)$, 但这与 $a_1,a_2,\cdots,a_n$ 不全为零矛盾, 所以由反证法原理可知, $\left\{\dfrac{1}{x-u}|u\in\mathbf{R}\right\}$ 是 V 的线性无关集. ■

设 V 是一个有限维向量空间, 取定 V 的一组基 $e_1,e_2,\cdots,e_n$, 那么 V 中的每一个向量 u 都可唯一地表示成 $e_1,e_2,\cdots,e_n$ 的线性组合:

$$u=c_1e_1+c_2e_2+\cdots+c_ne_n.$$

可以证明有限维向量空间的基一定存在, 并且不同的基具有相同的元素个数.

定理 4.1.5 设 R 是一个交换整环, $F\subseteq R$, F 是 R 的一个域, 并且 R 看成是 F 上的向量空间时是有限维的, 则

(1) 对任意一个 $a \in R$, 一定存在某个非零多项式 $f(x) \in F[x]$, 使得 $f(a) = 0$.

(2) R 一定是域.

证明　(1) 设 R 是 n 维的向量空间, 则对任意 $a \in R$, $n+1$ 个元素 $1, a, a^2, \cdots, a^n$ 是线性相关的. 故存在不全为 0 的 $c_0, c_1, \cdots, c_n \in F$, 使得

$$c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n = 0.$$

取 $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$, 则 $f(x) \in F[x], f(a) = 0$.

(2) 明显地, 要证明 R 是一个域, 只要证明 R 中不为 0 的元素都是乘法可逆元. 对任意一个 $a \in R, a \neq 0$, 由 (1) 可知存在非零的多项式 $f(x) \in F[x], f(a) = 0$. 不妨设 $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m$ 是 $F[x]$ 中满足 $f(a) = 0$ 次数最小的多项式, 则 $c_0 \neq 0$, 不然的话, $g(x) = c_1 + c_2 x + \cdots + c_m x^{m-1} \in F[x]$ 为满足 $g(a) = 0$ 次数更小的多项式.

由于 $f(a) = c_0 + c_1 a + c_2 a^2 + \cdots + c_m a^m = 0$, 故

$$(c_1 + c_2 a + \cdots + c_m a^{m-1})a = -c_0.$$

由 $c_0 \neq 0$, $c_0 \in F$ 可知 c_0^{-1} 存在. 令 $b = (c_1 + c_2 a + \cdots + c_m a^{m-1})(-c_0)^{-1}$, 则 $ab = 1$, 因此 R 中不为 0 的元素都是乘法可逆元, 所以 R 是一个域. ■

5　线性映射

定义 4.1.6　设 V_1, V_2 是同一个域 F 上的两个向量空间, T 是从 V_1 到 V_2 的一个映射, 若 $T(au + bv) = aT(u) + bT(v)$ 对任意 $a, b \in F$ 和任意 $u, v \in V_1$ 成立, 则称 T 是线性映射. 线性映射也称为向量空间之间的同态, 当 $V_1 = V_2 = V$ 时, 一般将线性映射 T 称为线性变换. 当 $V_2 = F$ 时, 将线性映射 T 称为线性泛函.

明显地, 线性映射有下面的性质.

性质 4.1.3　设 F 是一个域, V 是 F 上的向量空间, 则对任意线性映射 T, 有 $T(0) = 0$, 并且 $T(au - bv) = aT(u) - bT(v)$ 对任意 $a, b \in F$ 和任意 $u, v \in V$ 成立.

例 4.1.10　设 $p(x)$ 和 $q(x)$ 为实数 $\mathbf{R}$ 上的连续函数, $C^2(-\infty, +\infty)$ 为所有的二阶可微函数, $C(-\infty, +\infty)$ 为所有的连续函数, 它们都是实数域 $\mathbf{R}$ 上的向量空间. 若定义

$$T(f)(x) = f''(x) + p(x)f'(x) + q(x)f(x),$$

则 T 是线性映射, 并且 $f \in \mathrm{Ker}(T)$ 的充要条件为 f 是微分方程 $y''+p(x)y'+q(x)y=0$ 的解.

不难理解, 若 T 是有限维向量空间 V 上的一个线性变换, 取定 V 的一组基 $e_1, e_2, \cdots, e_n$ 后, T 就确定了域 F 上的一个 $n \times n$ 矩阵. 域 F 上的矩阵的运算法则和实数域上的矩阵一样, 不过矩阵元素的四则运算要按域 F 中的运算进行. 关于矩阵的秩, 行列式等概念和定理都与实数域上的很类似.

4.2 内积空间

在空间解析几何中, 对于向量 $u, v \in \mathbf{R}^2$, 内积为 $u \cdot v = |u||v|\cos\theta$, 内积非常直观明了, 利用内积可以方便地讨论向量的正交性和投影等, 内积还可以推广到域上的向量空间.

1 内积的定义

定义 4.2.1 *设 F 是一个域, V 是 F 上的一个向量空间, 若存在 $V \times V$ 到 F 的一个映射, 使得对任意 $u, v, w \in V$, $a, b \in F$, 有*

(1) $(u, v) = (v, u)$;

(2) $(au + bv, w) = a(u, w) + b(v, w)$.

则称 V 为内积空间 (inner product space). *若对所有的 $u \in V$, 当 $(u, u) = 0$ 时一定有 $u = 0$, 则称该内积* (inner product) *是非退化的* (nondegenerate).

例 4.2.1 在平面 $\mathbf{R}^2$ 中, 把一个点看成一个向量, 在加法

$$u + v = (u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2)$$

和数乘

$$a(u_1, u_2) = (au_1, au_2)$$

下, $\mathbf{R}^2$ 是实数 $\mathbf{R}$ 上的向量空间, 对于任意两个点 $u = (u_1, u_2), v = (v_1, v_2)$, 定义内积

$$(u, v) = u_1v_1 + u_2v_2,$$

则 $\mathbf{R}^2$ 为内积空间, 容易知道该内积是非退化的.

例 4.2.2　$\mathbf{Z}_2$ 作为域 $\mathbf{Z}_2$ 上的向量空间时, 对任意两个点 $u=(u_1,u_2), v=(v_1,v_2)$, 定义内积

$$(u,v)=u_1v_1+u_2v_2,$$

则 $\mathbf{Z}_2$ 是内积空间, 但对于 $u=(\overline{1},\overline{1})$, 有 $(u,u)=0$, 因此该内积不是非退化的.

例 4.2.3　在向量空间 $C[a,b]=\{u(t)|u(t)$ 为 $[a,b]$ 上的连续函数 $\}$ 上, 定义

$$(u,v)=\int_a^b u(t)v(t)\mathrm{d}t,$$

则 $C[a,b]$ 是内积空间.

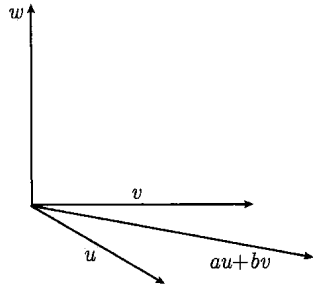
明显地, 内积有下面的性质.

性质 4.2.1　*设 F 是一个域, V 是 F 上的内积空间, 则对任意 $u\in V$, 有 $(u,0)=0$.*

2　正交和正交基

定义 4.2.2　*设 F 是一个域, V 是 F 上的内积空间, 若 $u,v\in V$, 有 $(u,v)=0$, 则称 u 和 v 是正交的* (orthogonal).

容易验证, 正交有下面的性质.



性质 4.2.2　*设 F 是一个域, V 是 F 上的内积空间, 若 $u,v,w\in V$, u 和 w 是正交的, 并且 v 和 w 也是正交的, 则对任意 $a,b\in F$, $au+bv$ 和 w 是正交的.*

定义 4.2.3　*设 F 是一个域, V 是 F 上的内积空间, 若 $u_1,u_2,\cdots,u_n\in V$ 为 V 的基, 并且对任意 $i\neq j$, 有 $(u_i,u_j)=0$, 则称 $u_1,u_2,\cdots,u_n\in V$ 为 V 的正交基* (orthogonal basis).

例 4.2.4　平面 $\mathbf{R}^n$ 是实数 $\mathbf{R}$ 上的向量空间, 对任意两个点 $u=(u_1,u_2,\cdots,u_n)$, $v=(v_1,v_2,\cdots,v_n)$, 内积 $(u,v)=u_1v_1+u_2v_2+\cdots+u_nv_n$, 则内积空间 $\mathbf{R}^n$ 有正交基 $u_1=(1,0,\cdots,0)$, $u_2=(0,1,\cdots,0),\cdots,u_n=(0,0,\cdots,1)$.

对于实数域 $\mathbf{R}$ 上的 n 维内积空间 $\mathbf{R}^n$, 容易知道存在正交基 $\{u_1,u_2,\cdots,u_n\}$, 并且对 $\mathbf{R}^n$ 的任意一组线性无关的元素, 都可以正交化. 任意域 F 上的 n 维内积空间也有类似的结论吗?

定理 4.2.1 设 F 是一个特征不为 2 的域, V 是 F 上的 n 维内积空间, 则 V 一定存在正交基 $\{u_1, u_2, \cdots, u_n\}$.

证明 (1) 若对任意的 $u \in V$, 都有 $(u,u) = 0$, 则任意取定 V 的一组基 $\{u_1, u_2, \cdots, u_n\}$, 由于 $(u_i + u_j, u_i + u_j) = 0$, 故

$$(u_i, u_i) + (u_i, u_j) + (u_i, u_j) + (u_j, u_j) = 0,$$

从而 $2(u_i, u_j) = 0$. 由 F 是一个特征不为 2 的域可知 $(u_i, u_j) = 0$, 因而 $\{u_1, u_2, \cdots, u_n\}$ 是 V 的正交基 $\{u_1, u_2, \cdots, u_n\}$.

(2) 若存在 $u_1 \in V, u_1 \neq 0$, 使得 $(u_1, u_1) \neq 0$, 取 $w_2, w_3, \cdots, w_n \in V$, 使得 $\{u_1, w_2, w_3, \cdots, w_n\}$ 是 V 的一组基. 令 $v_i = w_i - (u_1, u_1)^{-1}(u_1, w_i)u_1$, 则 $(u_1, v_i) = 0$ 对任意 $i > 1$ 成立, 因此对 $H_1 =< v_2, v_3, \cdots, v_n >$, 有 $(u_1, v) = 0, v \in H_1$.

(3) 在子空间 H_1 中, 若对任意 $v \in H_1$, 有 $(v, v) = 0$, 则由 (1) 的讨论容易知道 $i, j > 1$ 时, 有 $(v_i, v_j) = 0, i \neq j$.

(4) 若存在 $u_2 \in H_1, u_2 \neq 0$, 使得 $(u_2, u_2) \neq 0$, 用上面 (2) 的方法可以找到 $n-2$ 个元素 $w_3', \cdots, w_n'$, 使得 $\{u_2, w_3', \cdots, w_n'\}$ 是 H_1 的一组基, 从而存在 $v_3', \cdots, v_n' \in H_1$, 使得 $H_2 =< v_3', \cdots, v_n' >$, 有 $(u_2, v') = 0, v' \in H_2$, 因此 $u_1, u_2 \in V, (u_1, u_2) = 0$, 并且它们是线性无关的.

(5) 由于 V 是 F 上的有限维内积空间, 故经过上面方法的有限次重复, 一定可以找到 V 的一个正交基. ■

定理 4.2.2 设 F 是一个域, V 是 F 上的一个内积空间, 若 W 是 V 的一个子空间, 定义 W 的正交补 (orthogonal complement) 为 $W^{\perp} = \{v \in V | (u, v) = 0$ 对所有的 $u \in W$ 成立$\}$, 则 $W^{\perp}$ 为 V 的一个子空间.

证明 容易验证:

(1) $0 \in W^{\perp}$;

(2) $u + v \in W^{\perp}$ 对任意 $u, v \in W^{\perp}$ 成立;

(3) $au \in W^{\perp}$ 对任意 $a \in F, u \in W^{\perp}$ 成立;

所以, W 为 V 的一个子空间. ■

容易证明下面结论成立.

性质 4.2.3　若 V 是 F 上的一个内积空间，V_1 和 V_2 是 V 的子空间，并且 $V_1 \subseteq V_2$，则 $V_1^{\perp} \supseteq V_2^{\perp}$.

性质 4.2.4　若 V 是 F 上的内积空间，则 V 的内积是非退化的当且仅当 $V \cap V^{\perp} = \{0\}$.

3　赋范空间

数域上的向量空间还可以引入范数，使之成为泛函分析中的重要研究对象，Banach 在 1922 年定义范数和赋范空间.

定义 4.2.4　设 F 是实数域 $\mathbf{R}$ 或复数域 $\mathbf{C}$，V 是域 F 上的向量空间，若 $||\cdot||$ 是 V 到 $\mathbf{R}$ 的映射，且满足下列条件：

(1) $||u|| \geqslant 0$ 且 $||u|| = 0$ 当且仅当 $u = 0$;

(2) $||au|| = |a|||u||$，对任意 $u \in V$ 和任意 $a \in F$;

(3) $||u + v|| \leqslant ||u|| + ||v||$，对任意 $u, v \in V$.

则称 $||\cdot||$ 为 V 上的范数 (norm)，而 $||u||$ 称为 u 的范数，此时称 $(V, ||\cdot||)$ 为赋范空间 (normed space).

例 4.2.5　$C[0,1] = \{u(t) | u(t)$ 为 $[0, 1]$ 上的连续函数 $\}$，在范数 $||u|| = \sup\{|u(t)| | t \in [0,1]\}$ 下是赋范空间.

例 4.2.6　多项式环 $\mathbf{R}[x]$ 为实数 $\mathbf{R}$ 上的向量空间. 对任意

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbf{R}[x],$$

定义

$$||f|| = \max\{|a_n|, |a_{n-1}|, \cdots, |a_1|, |a_0|\},$$

则 $\mathbf{R}[x]$ 是赋范空间.

4.3　模

模是向量空间的直接推广，只要把域 F 换成任意一个环 R 就可以了. 模这种代数体系有很大的概括性，是一类基本和重要的代数体系，模在研究表示论、结构论方面都起着重要的作用.

1 模的定义

模最早是出现在 Dedekind 1870 年关于数论的工作中, 近代的模的理论来源于 Noether 和 Schmeider 在 1920 年的工作①和 Noether 在 1929 年的工作②.

定义 4.3.1 设 R 是一个环, M 是一个 Abel 群, 若有一个数乘运算

$$\begin{aligned} R \times M &\to M, \\ (a, u) &\mapsto au \end{aligned}$$

满足以下条件:

(1) $1u = u$ 对任意 $u \in M$ 成立;

(2) $(ab)u = a(bu)$ 对任意 $a, b \in R, u \in M$ 成立;

(3) $(a+b)u = au + bu$ 对任意 $a, b \in R, u \in M$ 成立;

(4) $a(u+w) = au + aw$ 对任意 $a \in R, u, w \in M$ 成立.

则称 M 为环 R 上的一个左模 (left module).

所谓左模是指用 R 的元素 a 从左边去乘 M 的元素 u. 同样地, 可以定义右模 (right module), 只需将上面条件 (1)~(4) 中 F 的元素写在 M 的元素 u 右边即可:

(1*) $u1 = u$ 对任意 $u \in M$ 成立;

(2*) $u(ba) = (ub)a$ 对任意 $a, b \in R, u \in M$ 成立;

(3*) $u(a+b) = ua + ub$ 对任意 $a, b \in R, u \in M$ 成立;

(4*) $(u+w)a = ua + wa$ 对任意 $a \in R, u, w \in M$ 成立.

一般来说, 环 R 上的左模 M 不一定是右模, 如取值于 $\mathbf{Z}_2$ 的矩阵加法群 $M = \left\{ \begin{bmatrix} 0 & u \\ 0 & v \end{bmatrix} | u, v \in \mathbf{Z}_2 \right\}$ 是非交换环 $R = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} | a, b, c \in \mathbf{Z}_2 \right\}$ 上的左模, 但它不是右模.

由于右模的理论与左模是完全平行的, 故只需讨论左模, 一般都将环 R 上的左模称为 R 上的模 (module). 除非特别说明, 后面出现的模都是指左模.

① Noether E, Schmeidler W. Moduln in nichtkommutativen Bereichen, insbesondere aus Differentialund Differenzenausdrücken. Math. Z., 1920, 8(1–2): 1–35.

② Noether E. Hyperkomplexe Größen und Darstellungstheorie. Math. Z., 1929, 30(1): 641–692.

2　模的性质

由模的定义, 容易知道下面性质成立.

性质 4.3.1　*若 M 是交换环 R 上的模, 则对任意的 $a \in R, u \in M$, 有*

$$a0 = 0, \quad 0u = 0, \quad a(-u) = (-a)u = -(au).$$

例 4.3.1　整数加法群 $\mathbf{Z}$ 可以看做整数环 $\mathbf{Z}$ 上的模.

例 4.3.2　加法 Abel 群 M 可以成整数环 $\mathbf{Z}$ 上的模, 因此模也可以看做 Abel 群的推广.

思考题 4.3.1　*若 M 是交换环 R 上的模, 对任意的 $a \in R, u \in M$, 当 $au = 0$ 时, 一定有 $a = 0$ 或 $u = 0$ 吗?*

不一定. 整数加法群 $\mathbf{Z}_6$ 可以看做整数环 $\mathbf{Z}_6$ 上的模, 但对于 $\overline{2} \in \mathbf{Z}_6$, $\overline{3} \in \mathbf{Z}_6$, 有 $\overline{2} \cdot \overline{3} = \overline{0}$.

性质 4.3.2　*若 R 是环, M 是它的一个左理想, 则 M 可以看做环 R 上的左模.*

定义 4.3.2　*若 M 是环 R 上的模, N 是 M 的子集, 若*

(1) *N 是 M 的子群;*

(2) *对任意 $a \in R, u \in N$, 有 $au \in N$ 成立.*

则称 N 是 M 的子模.

描述子模一般有效的方法就是生成的方法, 若 S 是模 M 的一个子集, 令

$$L(S) = \{a_1u_1 + a_2u_2 + \cdots + a_nu_n | a_i \in R, u_i \in S\},$$

则容易验证 $L(S)$ 是 M 的一个子模.

定义 4.3.3　*若 S 是模 M 的一个子集, $L(S) = \{a_1u_1 + a_2u_2 + \cdots + a_nu_n | a_i \in R, u_i \in S\}$, 则称 $L(S)$ 是 S 生成的一个子模, S 称为一个生成组. 若 S 为有限子集, 则称 $L(S)$ 是有限生成的. 若 S 为单点子集 $\{u\}$, 则称 $L(S)$ 是循环子模, u 称为生成元.*

由于向量空间已经有了线性相关的概念, 模也可以沿用向量空间线性相关性的概念, 但由于模定义中的 F 是环, 故模的线性相关性有它自己的特点.

思考题 4.3.2 若 M 是交换环 R 上的模, 对任意非零的 $u \in M$, u 一定是线性无关的吗?

例 4.3.3 整数加法群 $\mathbf{Z}_6$ 是交换环 $\mathbf{Z}_6$ 上的模, 对于 $\overline{5} \in \mathbf{Z}_6$, 不存在 $a \in \mathbf{Z}_6$, 使得 $a \cdot \overline{5} = \overline{0}$, 因此 $\overline{5}$ 是线性无关的. 但对于加法群 $\mathbf{Z}_6$ 中的非零元 $\overline{2}$, 有交换环中的 $\overline{3} \in \mathbf{Z}_6$, 使得 $\overline{2} \cdot \overline{3} = \overline{0}$, 故 $\overline{2}$ 是线性相关的, 所以模中的非零元不一定是线性无关的.

思考题 4.3.3 若 M 是交换环 R 上的模, 对于一组线性相关的元素, 则组中的元素一定可以由其他元素线性表出吗?

不一定. 在例 4.3.3 中, $\overline{2}$ 和 $\overline{3}$ 是线性相关的, 但 $\overline{2}$ 不能由 $\overline{3}$ 线性表出.

有了线性相关的概念, 还可以给出自由模的概念.

定义 4.3.4 若环 R 上的模 M 存在一个子集 S, 使得任意 $u \in M$ 都可以写成 S 中有限个元素的线性表示, 并且表示是唯一的, 则称 S 为模 M 在 R 上的一个基. 若模 M 有基, 则称 M 是 R 上的自由模.

容易知道, S 为模 M 在 R 上的一个基的充要条件为

(1) 对任意 $u \in M$, 存在 $u_1, u_2, \cdots, u_n \in S$ 和 $a_1, a_2, \cdots, a_n \in R$, 使得

$$u = a_1u_1 + a_2u_2 + \cdots a_nu_n.$$

(2) 对 $u_1, u_2, \cdots, u_n \in S$ 和 $a_1, a_2, \cdots, a_n \in R$, 若 $a_1u_1 + a_2u_2 + \cdots a_nu_n = 0$, 则一定有

$$a_1 = a_2 = \cdots = a_n = 0.$$

例 4.3.4 整数加法群 $\mathbf{Z}_6$ 是交换环 $\mathbf{Z}_6$ 上的模, 对于 $\overline{1} \in \mathbf{Z}_6$, 不存在非零元 $a \in \mathbf{Z}_6$, 使得 $a \cdot \overline{1} = \overline{0}$, 因此 $\overline{1}$ 是线性无关的, 容易知道 $\{\overline{1}\}$ 是 $\mathbf{Z}_6$ 的基, $\mathbf{Z}_6$ 是自由模.

与群的直积类似, 可以定义模的直积.

定义 4.3.5 设 M 是环 R 上的模, $M_1, M_2, \cdots, M_n$ 是 M 的子模, 若

(1) 对任意 $u \in M$, 都有 $u = u_1 + u_2 + \cdots + u_n$, 这里 $u_i \in M_i$.

(2) $M_i \cap (M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = \{0\}$.

则称 M 是 $M_1, M_2, \cdots, M_n$ 的直和, 记为 $M = \oplus M_i$.

例 4.3.5　整数加法群 $\mathbf{Z}_6$ 是交换环 $\mathbf{Z}_6$ 上的模, 容易知道 $M_1=\{\overline{0},\overline{3}\}$, $M_2=\{\overline{0},\overline{2},\overline{4}\}$ 是 $\mathbf{Z}_6$ 的子模, 并且 $M=M_1\cup M_2$.

利用模的直和, 可以得到自由模的刻画.

定理 4.3.1　*若 M 是环 R 上的模, 则 M 是自由模的充要条件为 M 和 R 的直和同构.*

证明　若 M 是自由模, $S=\{u_\alpha|\alpha\in A\}$ 为它的基, 则对任意 $u\in M$, 有 $u_{\alpha_1},u_{\alpha_2},\cdots,u_{\alpha_n}\in S$ 和 $a_{\alpha_1},a_{\alpha_2},\cdots,a_{\alpha_n}\in R$, 使得 $u=a_{\alpha_1}u_{\alpha_1}+a_{\alpha_2}u_{\alpha_2}+\cdots+a_{\alpha_n}u_{\alpha_n}$. 定义映射 $\varphi:M\to\oplus_\alpha R$, 则容易知道 φ 是同构. 反过来, 容易证明若存在同构 $\varphi:M\to\oplus_\alpha R$, 则 M 是自由模. ■

思考题 4.3.4　*若 M 是交换环 R 上的有限模, 则 M 中一定有线性无关的元素吗?*

不一定. 整数加法群 $\mathbf{Z}_6$ 是整数环 $\mathbf{Z}$ 上的模, 对任意 $u\in\mathbf{Z}_6$, $a\in\mathbf{Z}$, au 对 6 取模, 不难验证 $\mathbf{Z}_6$ 中的任意元素 u, 都存在 $a\in\mathbf{Z}$, 使得 $au=\overline{0}$, 因此 $\mathbf{Z}_6$ 中的任意元素 u 都不是线性无关的.

思考题 4.3.5　*若 M 是交换环 R 上的模, 则 M 中的非零元 u 都可以扩展成 M 的一组基吗?*

不一定. 实际上, 整数加法群 $\mathbf{Z}_6$ 是交换环 $\mathbf{Z}_6$ 上的模, 但非零元 $\overline{2}$ 是不可以扩展成 $\mathbf{Z}_6$ 的一组基的.

定理 4.3.2　*对于可除环 R 上的自由模 M, 若 $\{u_1,u_2,\cdots,u_m\}$ 和 $\{v_1,v_2,\cdots,v_n\}$ 都是 M 的基, 则 $m=n$.*

证明　不失一般性, 不妨假设 $m\geqslant n$, 由于 $\{u_1,u_2,\cdots,u_m\}$ 是 M 的基, 故存在 $a_1,a_2,\cdots,a_m\in R$, 使得 $v_n=a_1u_1+a_2u_2+\cdots+a_mu_m$. 设 k 是第一个使得 $a_k\neq 0$ 的下标, 则

$$u_k=a_k^{-1}v_n-a_k^{-1}a_1u_1-\cdots-a_k^{-1}a_{k-1}u_{k-1}-a_k^{-1}a_{k+1}u_{k+1}-\cdots-a_k^{-1}a_mu_m.$$

故 $\{v_n,u_1,\cdots,u_{k-1},u_{k+1},\cdots,u_m\}$ 生成 M. 因而存在 $b,b_1,b_2,\cdots,b_{i-1},b_{i+1},\cdots,b_m\in R$, 使得 $v_{n-1}=bv_n+b_1u_1+\cdots+b_{i-1}u_{i-1}+b_{i+1}u_{i+1}+\cdots+b_mu_m$. 由于 $\{v_{n-1},v_n\}$ 线性无关, 故 $v_{n-1}-bv_n\neq 0$. 设 j 是第一个使得 $b_j\neq 0$ 的下标, 则 u_j 是 v_{n-1},v_n 和 $u_i(i\neq k,j)$ 的线性组合, 故 $\{v_{n-1},v_n\}\cup\{u_i|i\neq k,j\}$ 生成 M, 从而 v_{n-2} 是 v_{n-1},v_n 和 $u_i(i\neq k,j)$ 的线性组合. 重复上面的步骤, 假如 $n<m$, 则 n 步

后, 可知 $\{v_n, v_{n-1}, \cdots, v_{m-n+1}\}$ 生成 M, 从而 v_{m-n} 是 $v_n, v_{n-1}, \cdots, v_{m-n+1}$ 的线性组合, 但这与 $\{v_1, v_2, \cdots, v_n\}$ 线性无关矛盾, 所以 $n = m$. ■

可以证明, 对于交换环 R 上的模 M, 基中元素的个数也是固定的, 下面定理也是成立的.

定理 4.3.3 对于交换环 R 上的自由模 M, 若 $\{u_1, u_2, \cdots, u_m\}$ 和 $\{v_1, v_2, \cdots, v_n\}$ 都是 M 的基, 则 $m = n$.

思考题 4.3.6 在什么条件下, 环 R 上的模 M 一定有一组基呢?

可以证明, 下面定理成立.

定理 4.3.4 若 M 是可除环 R 上的模, 则 M 一定有一组基.

进一步, 还有下面的结论成立.

定理 4.3.5 若 M 是可除环 R 上的模, 则 M 的任意一个线性无关集都一定可以扩展成 M 的一组基.

习 题 四

4.1 设 V 是闭区间 $[0, 2\pi]$ 上的连续函数全体所构成的向量空间, 试证明 x, $\sin x$, $\cos x$ 在 V 中线性无关.

4.2 试证明 $V = \left\{ \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \middle| a, b \in \mathbf{Z}_5 \right\}$ 是 $\mathbf{Z}_5$ 上的向量空间, 并求出 V 的一个基.

4.3 $V = \{(a_1, a_2) | a_1, a_2$ 为实数 $\}$ 是实数 $\mathbf{R}$ 上的向量空间, 问在 V 中是否存在一个内积, 使得 $(a, a) = 0$ 对所有的 $a = (a_1, a_2)$ 成立?

4.4 设 $\mathbf{Z}^2[x]$ 为 $\mathbf{Z}$ 上的次数小于等于 2 的多项式全体所构成的向量空间, 定义线性变换 T: $\mathbf{Z}^2[x] \to \mathbf{Z}^2[x]$, $T : f(x) \mapsto f'(x) - f(0)$, 试求出 T 的核空间 $\mathrm{Ker}(T)$ 和像空间 $\mathrm{Im}(T)$ 的一个基.

4.5 $C[a, b] = \{x(t) | x(t)$ 为 $[a, b]$ 上的连续函数$\}$是一个向量空间, 若

$$M[a, b] = \{x(t) | x(t) \in C[a, b], 0 \leqslant \int_a^b x(t)\mathrm{d}x \leqslant 1\},$$

问 $M[a,b]$ 是 $C[a,b]$ 的子空间吗?

4.6 在 $\mathbf{Z}_{11}$ 上的多项式构成的向量空间 $\mathbf{Z}_{11}[x]$ 中, 对任意 $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, $g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \in \mathbf{Z}_{11}[x]$, 定义内积 $(f(x), g(x)) = a_nb_n + a_{n-1}b_{n-1} + \cdots + a_1b_1 + a_0b_0$(这里不妨设 $n \geqslant m$, 当 $i > m$ 时, 取 $b_i = 0$). 令

$$W = \{a_3x^3 + a_2x^2 + a_1x + a_0 | a_0, a_1, a_2, a_3 \in \mathbf{Z}_{11}\}.$$

试求 W 的正交补 $W^{\perp}$.

4.7 设 $\mathbf{R}$ 为实数域, $T: \mathbf{R}^3 \to \mathbf{R}^2, (x_1, x_2, x_3) \mapsto (x_1 + x_2, x_1 - x_2)$, 试证明 T 是线性变换, 并求 $u, v, w \in \mathbf{R}^3$, 使得 $Tu = (1,0)$, $Tv = (0,1)$ 和 $Tw = (0,0)$.

4.8 整数加法群 $\mathbf{Z}_6$ 是交换环 $\mathbf{Z}_6$ 上的模, 试证明 $\bar{2}$ 和 $\bar{3}$ 是线性相关的.

4.9 设 F 是一个域, V 是 F 上的一个向量空间, 若 $\{u_1, u_2, u_3\}$ 是 V 的一个线性无关集, 试证明 $\{u_1 + u_2, u_2 + u_3, u_1 + u_3\}$ 是 V 的一个线性无关集的充要条件为域 F 的特征不是 2.

4.10 设 M 是交换环 R 的理想, 则 M 是交换环 R 上的模, 试证明任意非零元 $a, b \in M$, a 和 b 都是线性相关的.

4.11 若 M 是环 R 上的模, N 是 M 的非空子集, 试证明 N 是 M 的子模的充要条件为对于任意 $a, b \in R, u, v \in N$, 有 $au + bv \in N$ 成立.

～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～

阿廷 (E.Artin)1898 年 3 月 3 日生于奥地利的维也纳, 1921 年在莱比锡大学获博士学位. 在他的博士论文中, 他应用有理数域上的二次数域的算术以及解析理论来研究有限域上单变量有理函数域的二次扩张.1937 年移居美国.1937-1958 年先后在圣母大学、印第安纳大学、普林斯顿大学工作, 1958 年回汉堡大学. 阿廷是公认的近世抽象代数的奠基者之一, 阿廷前期工作主要是在类域论、实域理论、抽象代数等方面. 类域论是代数数论的重要分支, 是希尔伯特一手创造的. 阿廷在数学上最初的贡献是在代数数论方面, 而顶峰则是类域论的完成. 阿廷最重要的工作是一般互反律, 他给出了一般互反律的直接证明. 这不仅补充了类域论, 而且成为了其中的核心部分, 使他完全解决希尔伯特第 9 问题. 1925 年以后, 在诺特工作的启发下, 他开始了一些纯代数的工作, 他创造了"辫子理论", 引入辫子群, 把辫子的每根

头发相互缠绕的复杂关系变成一套漂亮的拓扑与群论理论. 在环论方面, 他把魏德伯恩 (Wedderburn) 著名的超复系的结构定理推广到具有链条件的结合环上, 这些环的理论满足升链条件与降链条件. 阿廷在抽象代数学方面最辉煌的业绩可以说是建立实域理论, 并由此完全解决希尔伯特的第 17 个问题.

学习指导

本章重点

1. 向量空间的线性无关和基.

2. 若 V 是无限域 F 上的向量空间, 则 V 不可能是有限个真子空间的并.

基本要求

1. 向量空间.

(1) 复习平面 $\mathbf{R}^2$ 中向量的运算和内积.

(2) 线性无关和基.

(3) 向量空间的子空间.

2. 内积的定义.

3. 模和子模的定义.

释疑解难

1. 向量空间的内积与空间解析几何中三维欧几里德空间 (Euclidean Space) 的内积不一样的就是: 一般来说 $u \in V$, 当 $(u,u)=0$ 时, 不一定有 $u=0$.

2. 当 V 是域 F 上的向量空间时, 讨论的都是 $a \in F$ 左乘 $u \in V$, 那 $a \in F$ 右乘 $u \in V$ 有意义吗? 因为数乘是 $F \times V$ 到 V 的运算, 所以 ua 没有任何意义.

3. 若 G 是交换加法群, 则对任意 $a \in G$ 和整数 $n \in \mathbf{Z}$, 有 $na \in G$, 并且 $(mn)a = m(na), (m+n)a = ma+na, m(a+b) = ma+mb$, 对任意 $m,n \in \mathbf{Z}$, $a,b \in G$

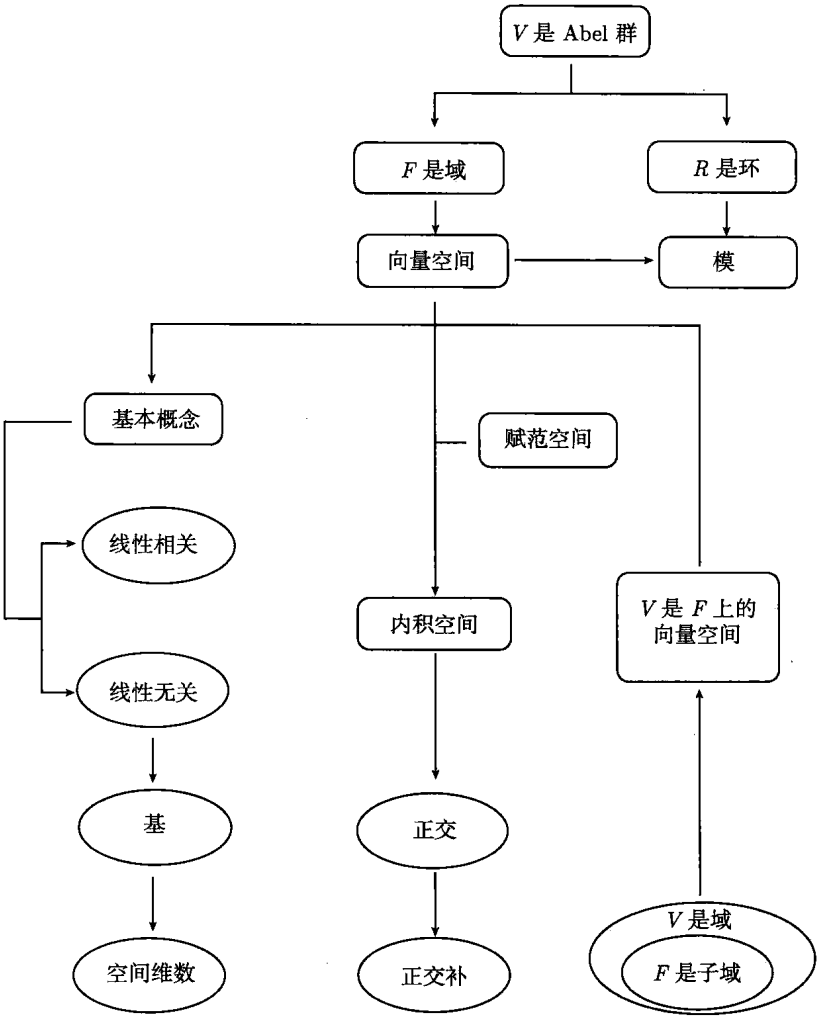
成立. 因此任意交换加法群 G 都可以看做整数上的左模. 所以, 模也可以看做是交换加法群概念的推广.

4. 由于模与线性空间有着比较类似的结构, 故有些证明可以类比, 如设 M_1, M_2 是环 R 上的模 M 的两个真子模, 一样可以类似证明 $M \neq M_1 \cup M_2$.

解题技巧

主要掌握在线性空间和模中, 如何判断几个向量是否线性无关的方法.

知识点联系图


V 是 Abel 群
F 是域
R 是环
向量空间
模
基本概念
赋范空间
线性相关
内积空间
V 是 F 上的向量空间
线性无关
基
正交
V 是域
F 是子域
空间维数
正交补

第 5 章　Sylow 定理和可解群

代数不过是书写的几何, 而几何不过是图形的代数.

Germain (1776—1831, 德国数学家)

由 Lagrange 定理可知, 有限群 G 的任意子群的阶是 $|G|$ 的因子. 反过来, 对于 $|G|$ 的因子 m, 是否存在一个 m 阶子群呢? 容易知道对有限循环群是成立的. 但交错群 A_4 的阶是 12, 它没有 6 阶子群, 因此 Lagrange 定理的逆命题是不成立的. 不过 A_4 有 2 阶、3 阶和 4 阶子群, 6 是两个素数 2 与 3 的乘积, 2, 3 和 4 都是一个素数的方幂, 因此自然会考虑: 若 $|G|$ 的因子 m 是一个素数的方幂时, 是否一定存在 m 阶子群呢?Sylow 定理回答了该问题, Sylow 定理是有限群理论最基本的定理之一, 它给出了有限群和它的子群之间深刻的联系.

5.1　群　作　用

设集合 $S=\{1,2,\cdots,n\}$, G 为 S 上的一个置换群, 任取 $g\in G$ 和 $x\in S$, 称 $g(x)$ 为群元素 g 对 x 的作用. 其实还可以将置换群对集合的作用推广到一般的群.

1　群作用的定义

定义 5.1.1　设 G 是一个群, S 是一个集合, 设有一个映射

$$\sigma: G\times S\to S$$

满足条件

(1) $\sigma(e,x)=x$ 对任何 $x\in S$ 成立;

(2) $\sigma(g_1g_2,x)=\sigma(g_1,\sigma(g_2,x))$ 对任何 $x\in S$ 和 $g_1,g_2\in G$ 成立.

则称 G 在 S 上有一个 (左) 作用 (action).

对于固定一个 $g \in G$, $x \mapsto \sigma(g,x)$ 给出从集合 S 到它自身中的一个映射. 因此用记号 gx 来代替 $x \mapsto \sigma(g,x)$ 更加简明. 但 gx 和群的乘法不同, g,x 分别在群 G 和集合 S 这两个不同的集合中, g 通常称为 "算子", $gx \in S$ 是 x 被 g 作用后的元素. 这样定义中的两个条件可以重新写成

(1) $ex = x$ 对任何 $x \in S$ 成立;

(2) $(g_1g_2)x = g_1(g_2x)$ 对任何 $x \in S$ 和 $g_1, g_2 \in G$ 成立.

条件 (2) 的左式中 g_1g_2 是群 G 中的乘法, 而右式中 $g_1(g_2x)$ 表示 x 被 g_2 作用后再被 g_1 作用. 由条件 (2) 得知, 记号 g_1g_2x 不会引起混淆.

右作用也可类似定义, 其满足的条件是:

(1) $xe = x$ 对任何 $x \in S$ 成立;

(2) $x(g_1g_2) = (xg_1)g_2$ 对任何 $x \in S$ 和 $g_1, g_2 \in G$ 成立.

性质 5.1.1 *设群 G 在 S 上有一个左作用, 则对任何 $g \in G$, 映射 $x \mapsto gx$ 是集合 S 到它自身的一个双射.*

证明 这是因为 $g^{-1}(gx) = (g^{-1}g)x = ex = x$.

下面是一些群作用的例子, 详细验证都很容易.

例 5.1.1 任何群 G 在任何集合 S 上有一个平凡的作用 $gx = x$.

例 5.1.2 G 在它自身上有一个左作用

$$G \times G \to G,$$

$$(g,a) = ga$$

称为**左平移**.

例 5.1.3 G 在它自身上有另一个左作用

$$G \times G \to G,$$

$$(g,a) = gag^{-1}$$

称为**共轭作用**, 一般直接用 gag^{-1} 来表示共轭作用.

后面如果没有说明群作用是左作用, 还是右作用的话, 群作用都是指左作用.

2　群作用的轨道和稳定子群

定义 5.1.2　设群 G 在集合 S 上有一个作用, 对于 $x \in S$, 集合

$$Gx = \{gx | g \in G\}$$

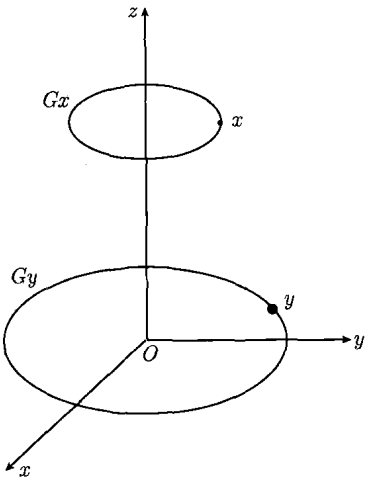
称为该作用的一条轨道 (orbit), 轨道中的元素个数称为该轨道的长度. 元素 $x \in S$ 的稳定子群 (stabilizer) 定义为

$$\mathrm{Stab}(x) = \{g \in G | gx = x\}.$$

容易验证 $\mathrm{Stab}(x)$ 确实是 G 的子群.

下面来看看群作用和轨道的一个比较直观的例子.

在直角坐标系中, 可以容易地看出, 如果取定OZ轴, 将围绕OZ轴按定向转动角 θ 的旋转全体记为 G. 即 $g \in G$ 时, 有 $0 \leqslant \theta < 2\pi$, 使得



$$g = \begin{bmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

明显地, G 在复合的运算下是一个群, 空间里的所有点记为 S, 则群 G 可以作用到空间 S 上. 取定空间 S 的一个点 x, 用群 G 作用点 x, 就可得到一个圆, 这就是 x 在 G 作用下的轨道 Gx.

3　轨道的性质

从左图中还可以看出, 轨道具有下面的性质.

性质 5.1.2　设 $x, y \in S$, 若 $Gx \cap Gy \neq \varnothing$, 则 $Gx = Gy$.

证明　设 $g_1 x = g_2 y$, 则 $g_1^{-1} g_2 y = x$. 对任意 $g \in G$, 有 $gx = g g_1^{-1} g_2 y \in Gy$. 故 $Gx \subseteq Gy$. 同理 $Gy \subseteq Gx$ 也成立, 所以 $Gx = Gy$. ■

这个结论表明, 两个轨道要么不相交, 要么重合. 而 S 中, 任一元都在某一个轨道内, 因此 S 可以表示成为不相交的诸轨道之并, 也就是说 G 作用在集合 S 上的轨道给出了 S 的一个划分.

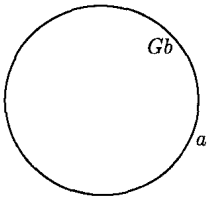
定义 5.1.3　只有一条轨道的群作用称为是可迁的 (transitive).

例 5.1.4 在它自身上的左平移是群 G 在 G 上的作用

$$G \times G \to G,$$

$$(g, a) = ga,$$

容易知道, 对于 G 中任意的 a 和 b, 有 $g = ab^{-1}$, 使得 $a = gb$, 故 $a \in Gb$. 由于 $a \in Ga$, 故 $Ga \cap Gb \neq \varnothing$, 因此 $Ga = Gb$. 所以群的左平移作用是可迁的.



由于 G 作用在集合 S 上的轨道给出了 S 的一个划分, 故集合 S 是有限集时, 每个轨道只含有有限个元素, 那么每个轨道究竟含有多少个元素呢? 实际上, 轨道 Gx 的元素个数和稳定子群 $\mathrm{Stab}(x)$ 有着密切的关系.

定理 5.1.1 设有限群 G 作用在集合 S 上, x 属于 S, 则

$$|Gx| = \frac{|G|}{|\mathrm{Stab}(x)|} = [G : \mathrm{Stab}(x)].$$

证明 设 $H = \mathrm{Stab}(x)$, G/H 为 H 的左陪集全体, 定义映射 $\varphi : Gx \to G/H$ 为 $\varphi(gx) = gH$. 若 $gx = g_1x$, 则 $g^{-1}g_1x = x$, 即 $g^{-1}g_1 \in H$, 因此 $gH = g_1H$, 因而 φ 的定义是合理的.

明显地, 对任意的 $gH \in G/H$, 有 $gx \in Gx$, 使得 $\varphi(gx) = gH$, 故 φ 是满射. 如若 $gH = g_1H$, 则 $g^{-1}g_1 \in H = \mathrm{Stab}(x)$, 因此 $g^{-1}g_1x = x$, 即 $g_1x = gx$, 因而 φ 是单射, 故 φ 是双射, 因此 $|Gx| = |G/H|$, 所以由 $|G| = |G/H| \cdot |H|$ 可知 $|Gx| = \dfrac{|G|}{|\mathrm{Stab}(x)|}$. ■

4 对称变换群

下面通过例子来说明群作用在研究对称变换中的应用.

使图形不变形地变到和它自身重合的变换称为这个图形的对称变换 (symmetric transformation). 一个图形的一切对称变换关于变换的乘法构成的群称为这个图形的对称变换群.

从下页图容易看出, 蝴蝶的对称变换只有左右对称变换和恒等变换两个, 因此蝴蝶对称变换群为左右对称变换和恒等变换构成的群.

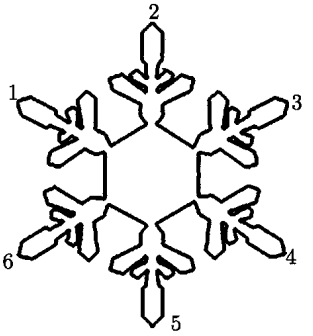
可以用群作用的方法来求对称变换群 G 的阶数.

例 5.1.5　试求冰花的对称变换群 G 的阶数.

解　冰花的六个花瓣分别用 1, 2, 3, 4, 5, 6 来编号. 令

$$S = \{1, 2, 3, 4, 5, 6\},$$

则冰花的每一个旋转都导致了 S 的一个变换, 这就给出了对称变换群 G 在 S 的一个作用. 不难验证, 1 在 G 下的轨道 $G1 = S$, 并且 Stab(1) ={恒等变换, 以 1 和 4 为对称轴的对称变换}, 故 $|\mathrm{Stab}(1)| = 2$, 所以 $|G| = |G1| \cdot |\mathrm{Stab}(1)| = 12$.



5　有限群的类方程

定义 5.1.4　*设群 G 作用在集合 S 上, 在每个轨道中取一个代表元, 它们构成一个集合 $D = \{x_1, x_2, \cdots, x_n\}$, 则 S 是轨道 $Gx_1, Gx_2, \cdots, Gx_n$ 的不相交的并, 这样的一个集合 D 称为代表元全系.*

定理 5.1.2　*设群 G 作用在集合 S 上, 且 S 是有限集, $D = \{x_1, x_2, \cdots, x_n\}$ 为代表元全系, 则*

$$|S| = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)].$$

证明　实际上, 对于 $D = \{x_1, x_2, \cdots, x_n\}$, S 是轨道 $Gx_1, Gx_2, \cdots, Gx_n$ 的不相交的并, S 的轨道给定了 S 的一个划分, 故 $|S| = \sum_{i=1}^{n} |Gx_i|$.

由于 $|Gx_i| = [G : \mathrm{Stab}(x_i)]$, 故定理成立. ■

在第 1.5 节中已经知道: 设 a, b 是群 G 的元素, 若存在 $g \in G$ 使得 $a = gbg^{-1}$, 则称 a 和 b 共轭, b 是 a 的共轭元.

容易验证共轭是 G 的等价关系, 因此等价关系决定 G 的一种分类, 群 G 可以划分为若干共轭类.

例 5.1.6 试写出 S_3 的共轭类.

解 容易知道 (1) 在 S_3 的共轭类只有它本身.

对于 $(12),(13),(23)\in S_3$, 由于

$$(23)(13)(23)^{-1}=(12),$$

$$(12)(23)(12)^{-1}=(13),$$

故 $(12),(13),(23)$ 在同一个共轭类内.

对于 $(123),(132)\in S_3$, 由于 $(12)(123)(12)^{-1}=(132)$, 故 (123) 和 (132) 在同一个共轭类内.

因为 $(1),(12),(123)$ 互不同类, 所以 S_3 的共轭类有三个:

$$\{(1)\},\{(12),(13),(23)\}\text{ 和 }\{(123),(132)\}.$$

考虑 G 在它自身上的共轭作用

$$G\times G\to G,$$

$$(g,a)=gag^{-1},$$

则对于 $x\in G$, 轨道为 $Gx=\{gxg^{-1}|g\in G\}$. 并且容易验证, x 属于 G 的中心时, $Gx=\{x\}$, 即共轭类只含一个元素 x. 另外, 对于 x 的稳定子群 $\mathrm{Stab}(x)$, 有

$$\begin{aligned}\mathrm{Stab}(x)&=\{g\in G|gxg^{-1}=x\}\\&=\{g\in G|gx=xg\}.\end{aligned}$$

因此, x 的稳定子群 $\mathrm{Stab}(x)$ 就是 x 在 G 中的中心化子 $C(x)$. 利用 x_i 在 G 中的中心化子 $C(x_i)$, 可以得到 $|G|=\sum_{i=1}^{n}|Gx_i|$ 新的表达形式.

下面定理是有限群的基本定理之一, 通常称定理中的式子为有限群的类方程.

定理 5.1.3 *设 G 是一个有限群, C 是 G 的中心, 则*

$$|G|=|C|+\sum_{i=1}^{n}[G:C(x_i)],$$

这里 $C(x_i)$ 表示 x_i 在 G 中的中心化子, x_i 取遍 G 中至少含有两个元素的共轭类全体.

证明　考虑 G 对 G 的共轭作用, 则 G 中元素 x 的轨道 $Gx=\{gxg^{-1}|g\in G\}$ 为所有与 x 共轭的元素全体, 当 x 属于 G 的中心时, x 的共轭类为 $\{x\}$. 因此只含有一个元素的共轭类的并集就是 G 的中心 C.

另外, 由于 $\mathrm{Stab}(x_i)=\{g\in G|gx_ig^{-1}=x_i\}=\{g\in G|gx_i=x_ig\}$, 因此 $\mathrm{Stab}(x_i)$ 就是 x_i 在 G 中的中心化子 $C(x_i)$, 由前面定理的结论 $|G|=\sum_{i=1}^{n}|Gx_i|$ 可知

$$|G|=|C|+\sum_{i=1}^{n}[G:C(x_i)].$$ ■

6　p 群的定义

定义 5.1.5　若有限群 G 的阶等于 p^m, 其中 p 为素数, m 为正整数, 则称 G 是一个 p 群.

例 5.1.7　加法群 $\mathbf{Z}_5$ 和 $\mathbf{Z}_7\oplus\mathbf{Z}_7$ 分别为阶是 5 和 7^2 的 p 群.

对于 p 群, 有如下结论.

定理 5.1.4　任意 p 群的中心一定含有不止一个元素.

证明　由于 G 的阶等于 p^m, $[G:C(x_i)]$ 都是 p^m 的因子, 由群的类方程

$$|G|=|C|+\sum_{i=1}^{n}[G:C(x_i)]$$

可知, $|G|$ 和 $\sum_{i=1}^{n}[G:G(x_i)]$ 都能被 p 整除. 如果该群中心 C 只含有一个元素, 则 $|C|+\sum_{i=1}^{n}[G:G(x_i)]$ 将不能被 p 整除, 但这与 $|G|$ 被 p 整除矛盾, 所以中心 C 不止含有一个元素. ■

从上面的证明可以看出, 实际上, 任意 p 群 G 的中心 C 一定是一个 p 群.

群对集合的作用有许多应用, 如下面的例题.

例 5.1.8　若 p 是素数, 试证明 p^2 阶群一定是 Abel 群.

证明 反证法. 假设 G 是非交换群, 并且 $|G| = p^2$, 则由前面定理可知 G 的中心一定含有不止一个元素, 根据 Lagrange 定理可知 C 为 p 阶群. 由于中心 C 一定是正规子群, 故商群 G/C 有定义, 并且它的阶为素数 p, 从而 G/C 是循环群. 若 yC 是 G/C 的生成元, 则 G 的全体为 $\{ay^i|a \in C, 0 \leqslant i < p\}$, 明显地, G 中的元都是可交换的, 但这与 G 是非交换群矛盾, 所以由反证法原理可知 p^2 阶群 G 一定是 Abel 群. ■

7 群在几何中的应用

群作用在几何中也有广泛的应用, 实际上, Klein 在 1872 年提出了 "爱尔朗根纲领", 试图用变换群之下的不变性与不变量概念把各种几何学统一起来, 并把变换群作为几何学分类的基础, 按这种观点, 几何学就是研究图形 (某种元素的集合) 在某种变换群作用下保持不变的性质的学科. 变换群是指集合之间的映射在映射的复合下构成的群. 如全体即平移、旋转及其复合构成一个刚体变换群, 全体刚体变换加上反射仍是一个群, 全体拓扑变换也是一个拓扑群. 因此刚体变换群对应的就是通常的初等几何, 它研究图形在刚体变换群作用下的不变性质与不变量, 因此, 常常将它称为刚体几何或度量几何; 仿射变换群对应于仿射几何, 它研究图形的仿射变换群作用不变性与不变量; 射影变换群对应于射影几何, 它研究图形在射影变换群作用的不变性与不变量; 拓扑变换群对应于拓扑学, 它研究图形的拓扑在拓扑变换群作用的不变性与不变量. 如果某个变换群是另一变换群的子群, 那么, 这个群对应的几何学就是另一个群对应的几何学的子几何学. 如刚体几何学是仿射几何的子几何, 仿射几何是射影几何的子几何.

5.2 Sylow 定 理

Cauchy 在 1844 年证明了 Galois 的断言: 每个有限置换群, 如果素数 p 能整除它的阶, 那么它至少包含一个 p 阶子群.Cauchy 还曾经证明, 若有限群 G 的阶可被素数 p 整除, 则 G 一定包含一个或多个 p 阶子群. 挪威数学家 Sylow 推广了 Cauchy 的定理. Sylow 在 1872 年证明了 Sylow 定理, 给出了一类子群的存在性, 还讨论了它们的一些性质. Sylow 定理在群论中有着深远的影响, 它揭示了群的算术性质与结构性质之间的精巧的联系.


Peter Ludwig Mejdell Sylow (1832-1918)

1　p-Sylow 子群的定义

定义 5.2.1　设 G 是一个有限群, p 是一个素数, 若 $p^m||G|$, 并且 p^{m+1} 不能整除 $|G|$, 则 G 的 p^m 阶子群称为 G 的 p-Sylow 子群.

例 5.2.1　加法群 $\mathbf{Z}_{12}$ 有一个 2-Sylow 子群 $\{\bar{0},\bar{3},\bar{6},\bar{9}\}$, 一个 3-Sylow 子群 $\{\bar{0},\bar{4},\bar{8}\}$.

例 5.2.2　交错群 A_4 有一个 2-Sylow 子群,

$$\{(1),(12)(34),(13)(24),(14)(23)\}$$

有四个 3-Sylow 子群,

$$\{(1),(123),(132)\},\{(1),(124),(142)\},\{(1),(134),(143)\},\{(1),(234),(243)\}.$$

由 Lagrange 定理可知, 若 a 是群 G 中的元素, 则 $o(a)$ 一定整除 $|G|$. 反过来, 若 m 整除 $|G|$, 则是否一定含有 m 阶的元素呢? Cauchy 很早就考虑了类似的问题.

引理 5.2.1(Cauchy 引理)　设 G 是一个有限 Abel 群, p 是素数, 若 p 整除 $|G|$, 则 G 有一个阶为 p 的元素.

证明　设 $|G|=pm, m\geqslant 1$, 对 m 用数学归纳法证明.

(1) 若 $m=1$, 则 G 的阶为素数 p, 因此 G 是循环群, 因而 G 有一个阶为 p 的元素, 所以结论成立.

(2) 假设对小于 m 的 r, 若 $|G|=pr$, 则 G 有一个阶为 p 的元素.

(3) 下面证明对于 $|G|=pm$ 的 Abel 群 G, G 有一个阶为 p 的元素.

取 $a\in G$ 且 $a\neq e$, 若 a 的阶可被 p 整除, 即 $o(a)=pl$, 则 $b=a^l$ 的阶等于 p, 从而 G 有一个阶为 p 的元素.

若 a 的阶不能被 p 整除, 则 a 的阶与 p 互素, 故 $G/<a>$ 的阶比 $|G|$ 小, 并且由 Lagrange 定理可知, $G/<a>$ 的阶还可被 p 整除, 因此 $|G/<a>|=pr$, $r<m$.

由归纳假设可知, $G/<a>$ 有一个 p 阶元 $b<a>$, 若 b 的阶为 s, 则

$$(b<a>)^s=b^s<a>=\bar{e}.$$

而 $b<a>$ 的阶等于 p, 故 $p|s$. 设 $s=pt$, 则 $c=b^t$ 的阶就是 p, 所以 G 有一个阶为 p 的元素.

由归纳法可知, 对任意的有限 Abel 群, 若 p 整除 $|G|$, 则 G 一定有一个 p 阶的元素. ■

实际上, Cauchy 引理对于非交换的有限群 G 也是成立的. 即*设 G 是一个有限群, p 是素数, 若 p 整除 $|G|$, 则 G 有一个阶为 p 的元素.*

2 Sylow 定理

Sylow 给出了进一步的结果, 他和 Cauchy 的结果可以说明 Lagrange 定理较弱的逆命题是成立的.

定理 5.2.1(Sylow 第一定理) *设 G 是一个有限群, p 是一个素数, 若 p^k 整除 $|G|$, 则 G 有一个阶为 p^k 的子群.*

证明 对群的阶 n 用数学归纳法来证明.

(1) 若 $n=2$, 则只有素数 2 整除 n, 明显地, G 就是一个 2-Sylow 子群, 因此结论成立.

(2) 假设结论对于一切阶小于 n 的群 G 成立, 即若 p^k 整除 $|G|$, 则 G 有一个阶为 p^k 的子群.

(3) 对于 n 阶的群 G, 可分情况来讨论 G 的类方程 $|G|=|C|+\sum[G:C(y_i)]$.

情形一. 如果 p 不能整除 $|C|$, 由 G 的类方程 $|G|=|C|+\sum[G:C(y_i)]$ 可知, 一定存在某个 i, 使得 p 不能整除 $[G:C(y_i)]$, 否则 p 不能整除 $|G|$.

由于 $|G|=|C(y_i)|[G:C(y_i)]$, $p^k||G|$, p 不能整除 $[G:C(y_i)]$, 因此 $p^k||C(y_i)|$. 明显地, G 的子群 $C(y_i)$ 的阶小于 $|G|$, 由归纳假设可知, $C(y_i)$ 含有一个 p^k 子群 H, 显然 H 也是 G 的子群, 因此 G 有一个阶为 p^k 的子群 H.

情形二. 如果 p 整除 $|C|$, 由 Cauchy 引理, C 一定含有一个 p 阶子群 $<c>$.

由于 $<c>$ 包含于中心 C, 故 $<c>$ 是 G 的正规子群, 并且 $G/<c>$ 的阶为 $\frac{1}{p}|G|$, 它可被 p^{k-1} 整除. 又因为 $G/<c>$ 的阶小于 $|G|$, 所以由归纳假设 $G/<c>$ 含有一个 p^{k-1} 阶子群 $H/<c>$, 因而 $|H|=[H:<c>]|<c>|=p^{k-1}\cdot p=p^k$, 因此 G 有一个阶为 p^k 的子群 H.

综合上述, G 一定包含一个阶为 p^k 的子群. ■

Sylow 在 1872 年给出的定理还给出了 Sylow 子群的性质和个数①.

定理 5.2.2(Sylow 第二定理)　*设 G 是有限群, p 为素数, 则 G 的任意两个 p-Sylow 子群都共轭.*

定理 5.2.3(Sylow 第三定理)　*设 G 是一个 p^nm 阶的有限群 (p 和 m 互素, $n \geqslant 1$), 则 G 的 p-Sylow 子群的个数为 $kp+1, k \geqslant 0$, 并且 $kp+1$ 整除 m.*

推论 5.2.1　*设 G 是有限群, p 为素数, 则 G 的每个 p^k 阶子群都包含在某个 p-Sylow 子群内.*

Sylow 定理有很多不同的证明, 如 Searcoid 的证明基于双陪集②. 还有用 Cauchy 引理来证明的, 不过 Wielandt 给出了没有用到 Cauchy 引理的证明③.

由于群 G 的任意两个 p-Sylow 子群都共轭, 故容易知道下面结论成立.

推论 5.2.2　*有限群 G 只有唯一的 p-Sylow 子群的充要条件为群 G 有一个 p-Sylow 正规子群.*

利用 Sylow 子群的正规化子可以研究群的结构. 1986 年, Bianchi, Mauri 和 Hanck 证明了: 如果有限群 G 的任意 Sylow 子群的正规化子幂零, 则群 G 本身是幂零的④. 1988 年, Fedri 和 Sereus 指出: 存在有限群 G, 它的每个 Sylow 子群的正规化子超可解, 但 G 本身不是超可解⑤.

Chigira, Iiyori 和 Yamaki 在 2000 年证明了: 若有限群 G 没有任何阶为 $2p$ 的元素 (p 为素数), 则 G 的 p-Sylow 子群都是交换的⑥.

3　Sylow 定理的应用

Sylow 定理是研究有限群的有力工具, 下面举例说明它的应用. 下面问题在讨论群的结构前, 应该先弄清楚.

① Sylow M L. Théorèmes sur les groupes de substitutions. Math. Ann., 1872, 5(4): 584–594.

② Searcoid. A reordering of the Sylow theorems. Amer. Math. Monthly, 1987, 94(2): 165–168.

③ Wielandt H. Ein beweis für die existenz der sylowgruppen. Arch. Math., 1959, 10: 401–402.

④ Bianchi M, Mauri G B, Peter H. On finite groups with nilpotent Sylow-normalizers. Arch. Math. (Basel), 1986, 47(3): 193–197.

⑤ Fedri V, Serena L. Finite soluble groups with supersoluble Sylow normalizers. Arch. Math. (Basel), 1988, 50(1): 11–18.

⑥ Chigira N, Iiyori N, Yamaki H. Non-abelian Sylow subgroups of finite groups of even order. Invent. Math., 2000, 139(3): 525–539.

思考题 5.2.1 *若 p 和 q 是不同的素数, 则有限群 G 的 p-Sylow 子群和 q-Sylow 子群有不是单位元的相同元素吗?*

没有. 如果 a 是 G 的 p-Sylow 子群和 q-Sylow 子群的共同元素, 那么 a 的阶一定整除 p 和 q, 因此 a 一定是单位元.

思考题 5.2.2 *若 p 是素数, 则有限群 G 不同的 p-Sylow 子群的交集只含单位元吗?*

不一定. 如在 S_4 中, 由于 $|S_4| = 24 = 2^3 \cdot 3$, 则有

$$H = \{(1), (12)(34), (13)(24), (14)(23), (12), (34), (1423), (1324)\},$$

$$K = \{(1), (12)(34), (13)(24), (14)(23), (13), (24), (1432), (1234)\}$$

都是 2-Sylow 子群, 但它们的交集为

$$H \cap K = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

例 5.2.3 试证明 56 阶群一定不是单群.

证明 由于 7-Sylow 子群有 $1+7k$ 个, 并且 $1+7k$ 整除 8, 故 $k = 0$ 或者 $k = 1$. 如果 $k = 0$, 则 7-Sylow 子群一定是正规的, 从而 G 不是单群.

若 $k = 1$, 则 G 有 8 个 7-Sylow 子群, 由于 7 阶是循环群, 故任意两个不同 7-Sylow 子群的交为单位元, 因此 7 阶元共 $6 \times 8 = 48$ 个非单位元, $56 - 48 = 8$. 但 G 含有 2-Sylow 子群, 其阶为 $2^3 = 8$. 因此剩下的 8 个元构成 G 的唯一的一个 2-Sylow 子群, 由此可知, G 有一个正规的 2-Sylow 子群, 所以 G 不是单群. ■

例 5.2.4 设 p 是素数, n 为大于零的整数, 若 $1 < m < p, G$ 是一个 $p^n m$ 阶群, 试证明群 G 不是单群.

证明 设 r 是 G 的 p-Sylow 子群的个数, 则根据 Sylow 定理, 有 r 被 p 除余数为 1, 并且 r 整除 m. 由 $1 < m < p$ 可知 $r = 1$, 因而 G 的 p-Sylow 子群只有一个, 从而它是 G 的非平凡正规子群, 所以 G 不是单群. ■

Horowitz 在 1966 年利用 Galois 理论和 2-Sylow 证明了代数学基本定理①.

① Horowitz L. A proof of the "Fundamental theorem of algebra" by means of Galois theory and 2-Sylow groups. Nieuw Arch. Wisk., 1966, 14(3): 95–96.

4　有限单群的分类简介

有限单群类似于整数中的素数, 它对于群论有重要意义. 像数论中每一个合数都可以被分解为它的素数因子的乘积一样, 每一个有限群都可以唯一分解为一些单群的集合, 找出所有的有限单群的问题称为有限单群分类问题.

问题　能不能找出所有的单群? 能否确定哪些群是单群, 哪些群不是单群?

有限单群分类从最初取得突破到最终完成, 经过近 50 年的努力, 终于解决了该问题, 整个证明分布在 500 多篇论文中, 共 10000 到 15000 页①, 有限单群分类定理是 20 世纪数学家们得到的一个最基本的结果, 全部的有限单群是:

(1) 素数阶循环群;

(2) $n \geqslant 5$ 的交错群 A_n;

(3) Lie 型单群 (共 16 族);

(4) 26 个散在单群.

Brauer 是现代有限单群分类工作的先驱, 他 1954 年证明了关于对合的中心化子定理. Feit 和 Thompson 在 1962 年证明了关键的 Burnside 猜想 —— 所有非交换单群都是偶数个元素的.1972 年, Gorenstein 在芝加哥大学举办的群论会议上提出了一个解决分类问题的 16 步纲领, 按照 Gorenstein 的纲领, Aschbacher 从一条被称为分支定理出发, 得到了很多导致单群分类定理最后解决的成果. 1980 年, Griess 找到了 26 个散在单群的最后一个散在群. 同年, 整个有限单群分类定理的证明完成了. 2004 年, Aschbacher M. 和 Smith S. D. 发表了文章②. 进一步完善了有限单群分类的工作, 从而补上了分类定理最初证明的最后一处漏洞, 因此分类定理就是一个定理了.

5.3　可　解　群

为了研究非交换群的结构, Burnside 于 1900 年左右提出了一个著名的猜想:

① Gorenstein D, Lyons R, Solomon R. The classification of the finite simple groups. Mathematical Surveys and Monographs, 40.1. American Mathematical Society, Providence, RI, 1994.

② Aschbacher M, Smith S D. The classification of quasithin groups. I. Structure of strongly quasithin K-groups. Mathematical Surveys and Monographs, 111. American Mathematical Society, Providence, RI, 2004.

一个奇数阶群 G 一定存在一个正规子群列：

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G,$$

使得每个 $G_i/G_{i-1}(1 \leqslant i \leqslant n)$ 是交换群. 这个猜想对有限单群分类问题的研究起了重要的作用.

1 合成群列的定义

定义 5.3.1 *设 G 是一个群, 称 $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$ 为 G 的一个正规群列, $G_i/G_{i-1}(1 \leqslant i \leqslant n)$ 称为商因子. 如果每个商因子都是单群, 则该正规群列称为 G 的合成群列* (composition series).

容易验证, 加法群 $\mathbf{Z}_6$ 有合成群列 $\{\overline{0}\} \lhd \{\overline{0}, \overline{2}, \overline{4}\} \lhd \mathbf{Z}_6$ 和 $\{\overline{0}\} \lhd \{\overline{0}, \overline{3}\} \lhd \mathbf{Z}_6$.$S_3$ 有合成群列 $\{(1)\} \lhd \{(1), (123), (132)\} \lhd S_3$.

H 是 G 的一个极大正规子群是指在 H 和 G 之间没有其他的正规子群, 一个群可能有阶和结构不同的极大正规子群. 另外, 若商群 G/H 的阶是素数, 则 H 是 G 的一个极大正规子群.

容易证明 H 是 G 的一个极大正规子群当且仅当 G/H 是单群. 因此 $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$*是 G 的合成群列的充要条件为* $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$ *是 G 的一个正规群列, 并且 G_i 是 G_{i+1} 的极大正规子群.*

思考题 5.3.1 *任意的有限群是否一定有一个合成群列?*

若 G 不是单群, 假设 G_1 是 G 的极大正规子群, G_2 是 G_1 的极大正规子群, G_3 是 G_2 的极大正规子群等, 并且阶是严格下降的, 由于群 G 的阶是有限的, 故容易理解最后一定会达到只含单位元的群. 实际上, 有下面的结论成立.

命题 5.3.1 *任何一个有限群 G 都一定有合成群列.*

证明 对群的阶 n 用归纳法来证明.

(1) 当 $n = 1$ 时, 若 G 的阶为 1, 则结论明显成立.

(2) 假设命题对于阶小于 n 的群都成立.

(3) 当 $|G| = n$ 时, 任取 G 的一个极大正规子群 G_{n-1}. 由于 G_{n-1} 是 G 的极大正规子群, $G_{n-1} \neq G$, G_{n-1} 和 G 之间没有其他正规子群, 因此 G/G_{n-1} 是单群.

明显地, $|G_{n-1}| < |G| = n$, 故由归纳假设 G_{n-1} 存在合成群列

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-2} \triangleleft G_{n-1}.$$

所以, $\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G$ 是 G 的合成群列. ■

思考题 5.3.2　*任意的无限群是否一定有一个合成群列?*

不一定.

例 5.3.1　整数加法群 $\mathbf{Z}$ 没有合成群列, 实际上, $\mathbf{Z}$ 的任何一个非平凡子群都与 $\mathbf{Z}$ 同构. 若 $\{0\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-2} \triangleleft G_{n-1} \triangleleft G = \mathbf{Z}$ 是 $\mathbf{Z}$ 的合成群列, 则 G_1 是 $\mathbf{Z}$ 的正规子群, 因此一定有整数 k_1, 使得 $G_1 = \{k_1 m | m \in \mathbf{Z}\}$, 从而 G_1 有正规子群 $H = \{2k_1 m | m \in \mathbf{Z}\}$, 但这与 $\{0\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-2} \triangleleft G_{n-1} \triangleleft G = \mathbf{Z}$ 是 $\mathbf{Z}$ 的合成群列意味着 $G_0 = \{0\}$ 一定是 G_1 极大正规子群矛盾, 所以整数加法群 $\mathbf{Z}$ 没有合成群列.

思考题 5.3.3　*任意的群如果有合成群列, 则它是否唯一呢?*

例 5.3.2　在四元数可除环中取 $\pm 1, \pm i, \pm j, \pm k$, 则它们在乘法下构成 8 阶非交换群 G.

令 $G_0 = \{1\}, G_1 = \{\pm 1\}, G_2 = \{\pm 1, \pm i\}, G_3 = G$, 则 $G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft G_3$ 是 G 的合成群列. 另外, 取 $H_0 = \{1\}, H_1 = \{\pm 1\}, H_2 = \{\pm 1, \pm j\}, H_3 = G$ 时, $H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft H_3$ 也是 G 的一个合成群列.

2　合成群列的性质

由于极大正规子群一般不是唯一的, 故一个有限群可能有不同的合成群列, 但它们有着密切的联系, 在重排和同构的意义下是唯一的, 这就是 Jordan-Hölder 定理.

定理 5.3.1(Jordan-Hölder 定理)　*设 G 是有限群, 下面两个群列都是 G 的合成群列:*

(1) $\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = G.$

(2) $\{e\} = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_s = G.$

则 $r = s$, 并且存在 $(1, 2, \cdots, r)$ 上的一个置换 σ, 使得

$$G_i / G_{i-1} \cong H_{\sigma(i)} / H_{\sigma(i)-1}.$$

证明 对群的阶 n 用数学归纳法.

(1) $n=1$ 时, 若群 G 的阶为 1, 则结论显然成立.

(2) 假设对阶小于 n 的群, 结论都成立.

(3) 若群 G 的阶为 n, 设有 G 的两个合成群列如下:

$$\{e\}=G_0\lhd G_1\lhd G_2\lhd\cdots\lhd G_r=G,$$

$$\{e\}=H_0\lhd H_1\lhd H_2\lhd\cdots\lhd H_s=G.$$

如果 $H_{s-1}=G_{r-1}$, 那么根据归纳假设, 由于 G_{r-1} 的阶比 G 的阶小, 故结论对 G_{r-1} 的两个合成群列成立, 而 $H_s=G_r=G$, 故结论显然对 G 也成立.

如果 $H_{s-1}\neq G_{r-1}$, 令 $K=H_{s-1}\cap G_{r-1}$, 由第二同构定理可知

$$G_{r-1}H_{s-1}/H_{s-1}\cong G_{r-1}/K.$$

但是 $G_{r-1}H_{s-1}$ 是真包含 H_{s-1} 的 G 的正规子群, 由 H_{s-1} 是 G 的极大正规子群知 $G_{r-1}H_{s-1}=G$. 故 $G/H_{s-1}\cong G_{r-1}/K$, 而 G/H_{s-1} 这是一个单群, 因此 G_{r-1}/K 也是单群, 即 K 是 G_{r-1} 的极大正规子群. 同理 K 也是 H_{s-1} 的极大正规子群. 设 K 的合成群列为

$$\{e\}=K_0\lhd K_1\lhd K_2\lhd\cdots\lhd K_m=K,$$

则可得到了 G 的两个合成群列:

$$\{e\}=K_0\lhd K_1\lhd K_2\lhd\cdots\lhd K_m\lhd G_{r-1}\lhd G,$$

$$\{e\}=K_0\lhd K_1\lhd K_2\lhd\cdots\lhd K_m\lhd H_{s-1}\lhd G.$$

比较下面的 2 个群列

$$\{e\}=G_0\lhd G_1\lhd G_2\lhd\cdots\lhd G_{r-1}\lhd G_r=G,$$

$$\{e\}=K_0\lhd K_1\lhd K_2\lhd\cdots\lhd K_m\lhd G_{r-1}\lhd G.$$

由于 G_{r-1} 的阶小于 n, 故由归纳假设可知 $r-2=m$. 并存在一个置换 σ, 使得

$$G_i/G_{i-1}\cong K_{\sigma(i)}/K_{\sigma(i)-1}.$$

同样地, 比较下面的 2 个群列.

$$\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_{s-1} \lhd H_s = G,$$

$$\{e\} = K_0 \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_m \lhd H_{s-1} \lhd G.$$

由于 H_{s-1} 的阶小于 n, 故由归纳假设可知 $s-2=m$. 并存在一个置换 τ, 使得

$$K_i/K_{i-1} \cong H_{\tau(i)}/H_{\tau(i)-1}.$$

由于

$$G/G_{r-1} = G_{r-1}H_{s-1}/G_{r-1} \cong H_{s-1}/K = H_{r-1}/K,$$

$$G_r/H_{s-1} = G_rH_{r-1}/G_{r-1} = G_{r-1}H_{r-1}/H_{r-1} \cong G_{r-1}/K,$$

于是 $r=s$, 并存在置换, 使得

$$G_i/G_{i-1} \cong H_{\tau\sigma(i)}/H_{\tau\sigma(i)-1} \quad (i = 1, 2, \cdots, r).$$

因此结论对阶等于 n 的群 G 成立. 所以, 由归纳原理可知定理成立. ■

实际上, 加法群 $\mathbf{Z}_6$ 有两个合成群列 $\{\overline{0}\} \lhd \{\overline{0}, \overline{2}, \overline{4}\} \lhd \mathbf{Z}_6$ 和 $\{\overline{0}\} \lhd \{\overline{0}, \overline{3}\} \lhd \mathbf{Z}_6$, 它们的长度一样, 并且 $\{\overline{0}, \overline{2}, \overline{4}\}/\{\overline{0}\} \cong \mathbf{Z}_6/\{\overline{0}, \overline{3}\}$, $\mathbf{Z}_6/\{\overline{0}, \overline{2}, \overline{4}\} \cong \{\overline{0}, \overline{3}\}/\{\overline{0}\}$, 因此加法群 $\mathbf{Z}_6$ 的两个合成群列是符合 Jordan-Hölder 定理的结论的.

3　可解群的定义

可解群与一元 n 次方程的可解性有关, 它是 Galois 引进的. 从 Galois 理论中可以知道, 因为 $n \geqslant 5$ 时 S_n 不是可解群, 所以五次及五次以上的代数方程才没有求根公式.

定义 5.3.2　*设 G 是一个群, 如果 G 具有一个正规群列, 其所有的商因子都是 Abel 群, 则 G 称为一个可解群* (solvable group).

可解群可以看做 Abel 群的推广, 它是一类非常重要的群.

设 G 是群, 为了简明, 以下都用 $G' = [G, G]$ 记 G 的换位子群, 容易证明换位子群 G' 一定是 G 的正规子群.

定义 5.3.3　*令 $G'' = (G')', \cdots, G^{(k)} = (G^{(k-1)})'$, 称 $G^{(k)}$ 为 G 的 k 次导群.*

容易知道, 群 G 是交换群当且仅当它的导群 $G'=[G,G]$ 是单位元. 导群是群交换性的一个反映, 从群的导群来研究群的性质或结构是群论研究的一个重要方面.

例 5.3.3 容易证明, 对称群 S_3 的 1 次导群为 $S_3'=A_3$, 2 次导群为 $S_3''=\{e\}$.

4 可解群的性质

利用 G 的 k 次导群, 可以得到可解群的一个判别法.

定理 5.3.2 *群 G 是可解群的充分必要条件是存在某个自然数 k, 使得 $G^{(k)}=\{e\}$.*

证明 若 $G^{(k)}=\{e\}$, 则有正规群列

$$\{e\}=G^{(k)}\triangleleft G^{(k-1)}\triangleleft\cdots\triangleleft G'=G.$$

并且每个 $G^{(i)}/G^{(i+1)}$ 都是 Abel 群, 因此 G 是可解群.

反过来, 若 G 可解, 则有下列正规群列:

$$\{e\}=G_0\triangleleft G_1\triangleleft G_2\triangleleft\cdots\triangleleft G_r=G,$$

使得 G_i/G_{i-1} 都是 Abel 群, 由于 $G_i'\subseteq G_{i-1}$, 故

$$G'\subseteq G_r'\subseteq G_{r-1},G_{r-1}'\subseteq G_{r-2},\cdots,$$

所以 $G^{(r)}=\{e\}$. ■

由此可见, 可解群可以看做 Abel 群的推广, G 为 Abel 群当且仅当 $G'=\{e\}$, k 次导群 $G^{(k)}=\{e\}$ 可以反映出可解群与 Abel 群的近似程度.

性质 5.3.1 *可解群的子群和同态像仍是可解群.*

证明 设 G 是可解群, H 是 G 的子群, 由于 H 是 G 的子群, 故 $H^{(i)}$ 是 $G^{(i)}$ 的子群, 因而 $G^{(k)}=\{e\}$ 时有 $H^{(k)}=\{e\}$, 所以 H 是可解群.

设 φ 是群 G 到 K 上的同态, 则 $\varphi(G')=K'$, 因而 $\varphi(G^{(k)})=K^{(k)}$. 由于 $G^{(k)}=\{e\}$, 故 $K^{(k)}=\{e\}$, 所以 K 也是可解群. ■

性质 5.3.2 *若 K 是群 G 的正规子群且 K 及 G/K 均是可解群, 则 G 也是可解群.*

证明　由于 K 及 G/K 均是可解群, 故存在 m 和 n, 使得

$$K^{(n)} = \{e\}, \quad (G/K)^{(m)} = \{e\},$$

由 $(G/K)^{(m)} = G^{(m)}/K$ 可知, $G^{(m)} \subseteq K$, 故 $G^{(m+n)} = \{e\}$, 所以 G 是可解群. ■

性质 5.3.3　*设 G 是一个有限群, 则*

(1) *若 M 和 N 都是 G 的正规子群, 并且 G/M 和 G/N 都是可解群, 则 $G/(M \cap N)$ 也是可解群.*

(2) *若 M 和 N 都是 G 的可解正规子群, 则 MN 也是 G 的可解正规子群.*

(3) *可解的单群一定是素数循环群.*

定理 5.3.3　*当 n 小于等于 4 时, S_n 是可解的.*

证明　S_1 的可解性是明显的.

S_2 有 $\{e\} \triangleleft S_2$, 并且 $|S_2/\{e\}| = 2$, 所以 S_2 可解. 由于 S_3 有一个 3 阶正规子群 A_3, 并且 $|A_3/\{e\}| = 3, |S_3/A_3| = 2$, 所以 S_3 可解. 对于 S_4, 令 $G_0 = \{e\}, G_1 = \{e, (12)(34), (13)(24), (14)(23)\}$, $G_2 = A_4, G_3 = S_4$. 则

$$G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft G_3$$

是 S_4 的正规群列, 其每个商因子是 Abel 群. ■

定理 5.3.4　*当 n 大于等于 5 时, S_n 是不可解群.*

证明　假设 S_n 是可解群, 则它的子群 A_n 也是可解群, 但当 $n \geqslant 5$ 时, A_n 是单群. 故 A_n 只有一个正规群列 $\{e\} \triangleleft A_n = G$, 但 $A_n/\{e\}$ 不是 Abel 群, 故 A_n 不是可解群, 矛盾. 所以 S_n 是不可解群. ■

利用 Jordan-Hölder 定理, 可导出有限群为可解群的判别定理.

定理 5.3.5　*设 G 是一个有限群, 则 G 是可解群的充分必要条件是 G 有一个合成群列:*

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = G,$$

其商因子 $G_i/G_{i-1} (1 \leqslant i \leqslant r)$ 皆为素数阶循环群.

证明　设 G 是可解群, 则它的任意一个合成群列的商因子一定是 Abel 群, 并且是单群, 从而必是素数阶循环群. 反过来, 如果 G 有一个合成群列其商因子为素数阶循环群, 则 G 明显地是可解群. ■

Burnside 证明了下面的定理.

定理 5.3.6 *对任意的素数 p,q, 任意一个阶为 p^aq^b 的群都是可解群.*

Feit 和 Thompson 在 1963 解决了 Burnside 猜想, 证明了下面群论中著名的奇阶定理①.

定理 5.3.7(Feit-Thompson 定理) *每一个奇数阶的有限群都是可解群.*

Feit 和 Thompson 的工作有 255 页, 占了 Pacific J. Math. 一期的版面, 他们两人获得了 1965 年的 Cole 奖. Thompson 并因后来关于极小单群的工作获得了 1970 年的 Fields 奖.

Isaacs, Navarro 和 Wolf 在 1999 年还证明了: 若 G 是可解群, a 有奇数阶, 则 a 一定在 Fitting 子群 $F(G)$ 中②.

习 题 五

5.1 试求出对称群 S_4 的所有可能的 Sylow 子群.

5.2 试求出 4 次交错群 A_4 的所有 Sylow 子群.

5.3 若 p 为素数, H 和 K 都是有限群 G 的阶为 p 幂的子群, 并且 H 是正规子群, 试证明HK也是 G 的阶为 p 幂的子群.

5.4 若有限群 G 的阶为 35, 试证明 G 一定是循环群.

5.5 试证明阶为 50 的群都一定有非平凡的正规子群.

5.6 设 G 是 168 阶的单群, 试确定 G 中所有阶为 7 的元素.

5.7 设 G 是 np 阶群 (p 为素数), 若 $n<p$, 试证明 G 有 p 阶的正规子群.

5.8 试证明 196 阶群 G 一定有一个阶大于 1 的 Sylow 子群, 它是 G 的一个正规子群.

---

① Feit W, Thompson J G. Solvability of groups of odd order. Pacific J. Math., 1963, 13: 775–1029.

② Isaacs I M, Navarro G, Wolf T R. Finite group elements where no irreducible character vanishes. J. Algebra, 1999, 222(2): 413–423.

5.9　设 G 是一个有限群, 若 $|G| = pqr$(这里 p, q, r 是不同的素数), 试证明 G 不是单群.

5.10　试证明 200 阶群 G 有正规的 Sylow 子群.

5.11　设 G 是一个有限群, 若 $|G| = pqr$(这里 p, q, r 是不一定不同的素数), 试证明 G 是可解群.

5.12　设 G 是一个 p^3 阶非交换群 (这里 p 是素数), 试证明 $C(G) = G'$.

5.13　试写出 Hamilton 四元素群的全部合成群列.

5.14　设 p, q 是不同素数, $p > q > 1$, 试证明 p^2q 群 G 一定是可解群.

5.15　试证明对称群 S_3 是可解群.

～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～

布饶尔 (R.Brauer)1901 年 2 月 10 日生于德国柏林, 童年时期一直过着无忧无虑、幸福快乐的生活, 1919 年入柏林大学学习, 在舒尔指导下于 1926 年 3 月完成博士论文. 毕业后在柯尼斯堡大学任教, 在柯尼斯堡的这段时间, 布饶尔对单代数的代数理论做出了重要贡献. 1931 年, 布饶尔、诺特和哈塞合作发表论文 "代数理论主定理的证明", 一举解决迪克森猜想, 完成代数主定理的证明. 1933 年因纳粹迫害犹太人移居北美, 先后在肯塔基大学 (1933—1934)、普林斯顿高等研究所 (任外尔的助手, 1934—1935)、多伦多大学 (1935—1948)、密歇根大学 (1948—1952)、哈佛大学 (1952—1971) 任教. 布饶尔在多伦多度过的那段时期是他最多产的一段时期, 他得到了许多重大成果, 其中的任何一个都足以使他居于一流数学家的行列. 1960 年之后, 布饶尔写了 50 多篇论文, 其中大多数属于模表示论及其应用. 布饶尔关于模表示的工作表现出其杰出的独创性, 他发展了这一理论, 发现并证明三个主要定理, 找到了它们在群论中的意想不到的深刻应用. 1955 年, 布饶尔和福勒发表了重要论文 "偶数阶群", 这篇论文非常简单, 任何知道群的定义的人都能理解其中的主要结果, 然而它们对偶数阶群论的大部分发展都非常重要. 布饶尔 1955 年当选为美国科学院院士, 1971 年获美国科学功绩奖章. 布饶尔在长达 50 年持续工作中, 对典型群表示论、单代数和分裂域、有限群模表示论、有限单群、代数数论等方面都作出了重要的贡献.

学习指导

本章重点

1. 群作用的性质和应用.

2. 三个 Sylow 定理.

3. 可解群的判断.

释疑解难

1. Sylow 定理对于 Sylow 子群的存在性、相互关系和个数都给予了完美的回答.

2. 由 Sylow 定理容易验证, 若 p 和 q 是不同的素数, 群 G 的阶为 pq, 并且 p 不能整除 $q-1$, q 也不能整除 $p-1$ 时, G 一定是循环群. 利用该结论, 可以判断阶为 15, 33, 35, 51, 65 等的群都是循环群.

3. 若 p 和 q 是不同的素数, 群 G 的阶为 pq 时, G 不一定是循环群. 如 $|S_3| = 2 \cdot 3$, 但它不是循环群.

4. 利用 Sylow 定理还可以确定一些群是不是单群. 如容易验证 196 阶群和 200 阶群都不是单群.

5. 利用 Sylow 定理还可以证明对有限交换群来说, Lagrange 定理的逆定理是成立的.

6. 若 $G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n$(这里 $G_0 = \{e\}, G_n = G$) 为群 G 的一个合成群列, 则 G_i 是 G_{i+1} 的正规子群, 但不要求 G_i 是 G_{i+2} 的正规子群, 也不要求 G_i 是 G 的正规子群.

7. 可解群的概念产生于描述其根可以只用根式 (平方根、立方根等及其和与积) 表示的多项式所对应的自同构群所拥有的性质, 因此它在 Galois 理论中是很重要的.

8. 所有的 Abel 群都是可解的.

9. 每一个奇数阶的有限群都是可解群.

解题技巧

1. 应用 Sylow 定理解题, 一般都按下面的步骤来讨论.

(1) 将有限群 G 的阶进行因子分解.

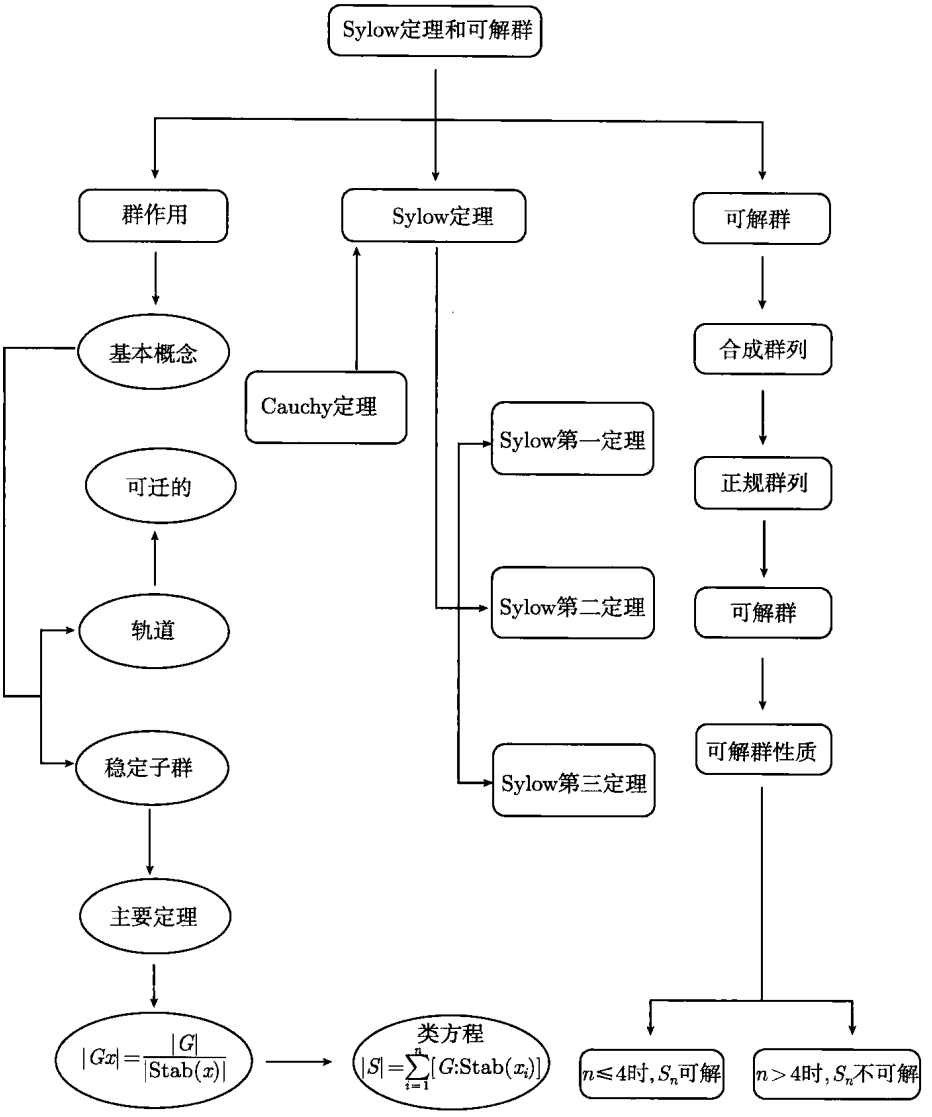
(2) 根据阶的因子分解, 应用 Sylow 定理, 得到的种类和个数等.

(3) 综合讨论, 得到所需的结论. 一般应注意如果群 G 只有唯一的 p-Sylow 子群, 那么它一定是群 G 的正规子群.

2. 若用 Sylow 定理可以证明群 G 只有唯一的一个素数 p 阶子群和另一个唯一的 q 阶子群 (这里 p 和 q 为不同素数), 并且没有其他的子群, 则它们都是正规子群, 并且交集为单位元, 所以 G 一定是循环群.

3. 要证明群 G 是可解群, 有时可以找出 G 的一个正规子群 H, 使得 H 和 G/H 都是可解群, 从而 G 是可解群. 例如, S_3/A_3 是 2 阶循环群, A_3 是 3 阶循环群, 因此 S_3/A_3 和 A_3 都是可解群, 所以 S_3 是可解群.

知识点联系图


Sylow定理和可解群
群作用
Sylow定理
可解群
基本概念
Cauchy定理
Sylow第一定理
合成群列
可迁的
正规群列
轨道
Sylow第二定理
可解群
稳定子群
Sylow第三定理
可解群性质
主要定理
$|Gx|=\frac{|G|}{|\mathrm{Stab}(x)|}$
类方程
$|S|=\sum_{i=1}^{n}[G:\mathrm{Stab}(x_i)]$
$n\leqslant 4$时，S_n可解
$n>4$时，S_n不可解

第6章　域的扩张

只要代数和几何沿着各自的途径去发展, 它们的进展将是缓慢的, 他们的应用也是很有限的. 但是, 当这两门学科结成伴侣, 它们都将从对方身上获得新鲜的活力, 因此, 以快速的步伐猛进, 趋于完美.

Lagrange (1735—1813, 法国数学家)

Évariste Galois (1811—1832)

历史上域扩张的研究主要来自研究代数方程可用根式求解的条件, Galois 于 1830 年前后彻底解决了这一问题. 他的出发点是, 将数域 F 上代数方程 $f(x)=0$ 左端多项式 $f(x)$ 的所有复根与 F 一起构成复数域 C 的一个子域, 并且使得这个子域是包含 $f(x)$ 的所有复根的域中最小的一个. Galois 理论的关键思想是: 对于域 K 的每个扩张 F, 都有一个由固定 K 中每个元素的 F 的自同构所构成的群. 域的 Galois 扩张可以用它的 Galois 群来定义, 或用该扩张的内部结构来定义. Galois 基本定理指出: 在域的 Galois 扩张的所有中间域和该域的 Galois 群的子群之间存在一一对应, 这样就可以将关于域、多项式和域的扩张的许多问题转化为群论的问题来考虑.

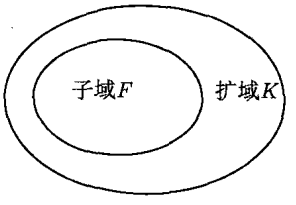
6.1　子域和扩域

研究域的一个方法就是从较小的域出发来构造较大的域, 这就是子域与扩域.

1　子域和扩域

定义 6.1.1　设 K 是域, F 是 K 的至少有两个元素的子集, 如果 F 关于 K 中的加法与乘法也构成一个域, 则称 F 是 K 的子域 (subfield), 此时也称 K 为 F 的扩域 (extension field). 用记号 K/F 表示 K 是 F 的域扩张.

例 6.1.1 实数域 $\mathbf{R}$ 是有理数域 $\mathbf{Q}$ 的扩域; 复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 的扩域, 也是有理数域 $\mathbf{Q}$ 的扩域.



一般地, 复数域的子域都称为数域 (number field).

例 6.1.2 设 i 是虚数单位, $\mathbf{Q}$ 是有理数域, 则 $F=\{a+bi|a,b\in\mathbf{Q}\}$ 是数域.

容易知道, 子域具有下面的性质.

性质 6.1.1 *设 F 是域, $K_i(i=1,2,\cdots,n,\cdots)$ 是 F 中的子域, 则 $K=\cap K_i$ 是 F 的一个子域.*

2 域的素子域和特征

定义 6.1.2 *设 F 是域, 则 F 的所有子域的交为 F 的最小的子域, 称为 F 的素子域* (prime subfield). *没有真子域的域一般称为素域* (prime field).

有理数域 $\mathbf{Q}$ 和 $\mathbf{Z}_p$ (p 为素数) 都是素域, 任意域的素子域本身可以看做一个素域. 容易理解, 任意域都可以看做它的素子域的扩域, 因此对域的扩张的研究有着普遍的意义.

设 R 是一个域, 若 R 没有周期元, 则该域的特征为零; 若 R 至少含有一个周期元, 则一定存在素数 p, 使得对 R 的一切非零元 r, 都有 $pr=0$, 这个 p 就是域 R 的特征. Steinitz 在 1910 年出版的名著《域的代数理论》(*Algebraische Theorie der Körper*) 中引进了域的特征, 把域按照特征分类, 他还引进了素子域、有限扩张、扩张次数等概念.

在第 2 章讨论整环和域的特征时, 已经证明下面结论成立.

定理 6.1.1 *设 F 是域, F_0 是 F 的素子域, 则当 F 的特征为素数 p 时, F_0 同构于有限域 $\mathbf{Z}_p$; 当 F 的特征为零时, F_0 同构于有理数域 $\mathbf{Q}$.*

因此, 从同构的观点来看, 任何域都不过是有理数域 $\mathbf{Q}$ 或 $\mathbf{Z}_p$ (p 为素数) 的扩域.

推论 6.1.1 *有理数域 $\mathbf{Q}$ 是最小的数域.*

明显地, 这是由于复数域 $\mathbf{C}$ 的特征是 0, 故它的素子域是有理数域 $\mathbf{Q}$.

3　集合 S 在 F 上生成的子域

若 F 是域 K 的子域, 考虑 F 在 K 有哪些扩张, 实际上, F 在 K 的扩张就是在 F 上添加一些 K 中的元素.

定义 6.1.3　设 K/F 是域扩张, S 是 K 中的非空子集, 则

$$F(S)=\cap\{L|L \text{ 是 } K \text{ 的子域, 并且 } S\subseteq L, F\subseteq L\}$$

是 K 中包含 F 与 S 的最小的子域, 称为集合 S 在 F 上生成的子域 (subfield generated by S over F), 也称为添加集合 S 到 F 得到的子域. 当 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$ 是有限集时, 就记为 $F(\alpha_1,\alpha_2,\cdots,\alpha_m)$.

4　单扩域

只添加一个元素的扩张是最简单的扩张.

定义 6.1.4　设 K/F 是域扩张, 如果有 $\alpha\in K$, 使得 $K=F(\alpha)$, 那么 K 称为 F 的单扩域 (simple extension field).

不过要注意的是, 一般来说, 当 F 为环时, $F[\alpha]$ 表示包含 F 和 α 的最小的环, 因此要注意符号 $F(\alpha)$ 与 $F[\alpha]$ 不要混淆了.

例 6.1.3　对于复数域 $\mathbf{C}$ 和实数域 $\mathbf{R}$, 有 $\mathrm{i}\in\mathbf{C}$, 使得 $\mathbf{C}=\mathbf{R}(\mathrm{i})$, 因此复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 的单扩域.

容易验证, 添加 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$ 到 F 得到的子域有如下的形式.

定理 6.1.2　设 K/F 是域扩张, $\alpha_1,\alpha_2,\cdots,\alpha_m\in K, L=F(\alpha_1,\alpha_2,\cdots,\alpha_m)$, 则

$$L=\left\{\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_m)}{g(\alpha_1,\alpha_2,\cdots,\alpha_m)}\middle|\ \text{这里 } f,g\in F[x_1,x_2,\cdots,x_m],\ \text{且 } g(\alpha_1,\alpha_2,\cdots,\alpha_m)\neq 0\right\}.$$

若 S 是两个集合的并集, 则有下面的结论成立.

定理 6.1.3　设 K/F 是域扩张, S_1,S_2 是 K 中的非空子集, $S=S_1\cup S_2$, 则

(1) 若 $S_1\subseteq S_2$, 则 $F(S_1)\subseteq F(S_2)$.

(2) $F(S)=F(S_1)(S_2)$.

证明 (1) 由上面定理 6.1.2 即知.

(2) 记 $H = F(S_1)(S_2)$. 由于 $F, S_1, S_2 \subseteq H$, 故 $F, S \subseteq H$, 从而有 $F(S) \subseteq H$. 另外, 由于 $F, S_1 \subseteq F(S)$, 因而有 $F(S_1) \subseteq F(S)$. 由 $S_2 \subseteq F(S)$ 可知 $H = F(S_1)(S_2) \subseteq F(S)$, 所以 $H = F(S)$. ■

由上面定理可知, 当 $S = \{\alpha_1\} \cup \{\alpha_2\}$ 时, 有 $F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2)$, 因此 K 在域 F 上一次添加有限个元素得到的扩域 $F(\alpha_1, \alpha_2, \cdots, \alpha_m)$, 可以由 F 添加一个元素得到 $F(\alpha_1)$, 然后继续添加得到 $F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2)$, 经有限次这样的添加而得到 $F(\alpha_1, \alpha_2, \cdots, \alpha_m)$.

5 域扩张的次数

设 K/F 是域扩张, 则 K 是 F 上的向量空间, 因此可以用向量空间的维数来讨论域扩张的性质.

定义 6.1.5 *设 K/F 是域扩张, 则 F 上的向量空间 K 的维数称为域扩张 K/F 的次数, 记为 $[K : F]$.*

例 6.1.4 对于复数域 $\mathbf{C}$ 和实数域 $\mathbf{R}$, $\mathbf{C}/\mathbf{R}$ 是域扩张, 由于 $\mathbf{R}$ 上的向量空间 $\mathbf{C}$ 的维数是 2, 因此 $\mathbf{C}/\mathbf{R}$ 的次数为 2.

明显地, 下面结论成立.

性质 6.1.2 *设 K 是 F 的扩域, 则 $[K : F] = 1$ 当且仅当 $K = F$.*

定义 6.1.6 *设 K/F 是域扩张, 若 $[K : F] < \infty$, 则 K 称为 F 的有限扩域或有限扩张* (finite extension field of F).

例 6.1.5 设 $H = \mathbf{Q}(\sqrt{2})$, 则有理数域 $\mathbf{Q}$ 上的向量空间 H 有基 $\{1, \sqrt{2}\}$, 因此有 $[H : \mathbf{Q}] = 2$. 若 $K = H(\sqrt{3}) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$, 则域 H 上的向量空间 K 有基 $\{1, \sqrt{3}\}$, 因此有 $[K : H] = 2$, 并且有理数域 $\mathbf{Q}$ 上的向量空间 K 有基 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, 所以 $[K : \mathbf{Q}] = 4$.

6 域扩张的次数公式

一般地, 有下面的结论成立. 这是在域论的主要定理之一, 起着与群论中的 Lagrange 定理相似的作用.

定理 6.1.4　*设 L 是 F 的扩域, K 是 L 的扩域, 则 K 是 F 的有限扩域当且仅当 L 是 F 的有限扩域, 且 K 是 L 的有限扩域. 此时有 $[K:F]=[K:L][L:F]$.*

证明　设 $n=[K:F]$, 则 K 中任何 $n+1$ 个元素在 F 上线性相关, 从而在 L 上也是线性相关的, 故 $[K:L]<\infty$. 同理可证 $[L:F]<\infty$.

反过来, 若 $[K:L]<\infty$ 且 $[L:F]<\infty$. 取 L 上的向量空间 K 中的基 $u_1,u_2,\cdots,u_s$ 及 F 上的向量空间 L 的基 $v_1,v_2,\cdots,v_m$. 对任何 $\alpha\in K$, 有

$$\alpha=\sum_{i=1}^{s}c_iu_i,\quad c_i\in L,\quad i=1,2,\cdots,s$$

及

$$c_i=\sum_{j=1}^{m}a_{ij}v_j,\quad a_{ij}\in F,\quad i=1,2,\cdots,s;\quad j=1,2,\cdots,m.$$

于是有 $\alpha=\sum\limits_{i=1}^{s}\sum\limits_{j=1}^{m}a_{ij}u_iv_j$, 即 K 中任何元素可由集合

$$S=\{u_iv_j|i=1,2,\cdots,s;j=1,2,\cdots,m\}$$

线性表示.

若

$$\sum_{i=1}^{s}\sum_{j=1}^{m}a_{ij}u_iv_j=\sum_{i=1}^{s}\left(\sum_{j=1}^{m}a_{ij}v_j\right)u_i=0,\quad a_{ij}\in F,$$

由于 $u_1,u_2,\cdots,u_s$ 是 K/F 的基, 因而

$$\sum_{j=1}^{m}a_{ij}v_j=0,\quad i=1,2,\cdots,s.$$

因此对所有的 i 与 j, 有 $a_{ij}=0$. 于是 S 在 F 上是线性无关的, 从而 S 是 F 上的向量空间 K 的基, 所以 $[K:F]=sm$. ■

由上面定理容易知道, 设 K 是 F 的有限扩域, 则 F 在 K 上的任意扩域 E 一定是有限扩域, 并且 $[E:F]$ 一定是 $[K:F]$ 的因子. 由此也可知道下面推论成立.

推论 6.1.2　*设 K/F 是域扩张, 且 $[K:F]$ 是素数, 则 F 与 K 之间再无其他的中间域.*

例 6.1.6　对于复数域 $\mathbf{C}$ 和实数域 $\mathbf{R}$, $[\mathbf{C}:\mathbf{R}]$ 是素数 2, 因此 $\mathbf{C}$ 与 $\mathbf{R}$ 之间再无其他的中间域.

例 6.1.7 对于实数域 $\mathbf{R}$ 和有理数域 $\mathbf{Q}$, 试证明 $\mathbf{R}$ 是 $\mathbf{Q}$ 的无限扩域.

证明 反证法. 假设 $[\mathbf{R}:\mathbf{Q}]$ 有限, 则由实数 $\sqrt[n]{3}$ 在 $\mathbf{Q}$ 上是多项式 x^n-3 的根, 容易验证

$$[\mathbf{R}:\mathbf{Q}]=[\mathbf{R}:\mathbf{Q}(\sqrt[n]{3})][\mathbf{Q}(\sqrt[n]{3}):\mathbf{Q}]=[\mathbf{R}:\mathbf{Q}(\sqrt[n]{3})]n,$$

故任意的 n 都整除 $[\mathbf{R}:\mathbf{Q}]$, 但这与 $[\mathbf{R}:\mathbf{Q}]$ 有限矛盾, 从而 $[\mathbf{R}:\mathbf{Q}]$ 一定是无穷, 所以 $\mathbf{R}$ 是 $\mathbf{Q}$ 的无限扩域. ■

6.2 代数扩张

若 K/F 是域扩张, $\alpha\in K$, 则 F 的单扩张为

$$F(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}\middle|\ \text{这里 } f,g\in F[x],\ \text{且 } g(\alpha)\neq 0\right\}.$$

因此单扩张 $F(\alpha)$ 的结构和代数性质与所添加的元素 α 的性质有关, 所以 α 与 F 之间的关系对研究单扩张 $F(\alpha)$ 的代数性质有着重要的意义.

1 代数元和超越元

定义 6.2.1 *设 K/F 是域扩张, $\alpha\in K$, 若 α 满足 F 上的一个代数方程*

$$a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n=0,$$

这里 a_i 不全为零, 则 α 称为 F 上的代数元 (algebraic element). *若 α 不是 F 上的代数元, 则 α 称为 F 上的超越元* (transcendental element).

定义 6.2.2 *有理数域 $\mathbf{Q}$ 上的代数元称为代数数* (algebraic number), *有理数域 $\mathbf{Q}$ 上的超越元称为超越数* (transcendental number).

性质 6.2.1 *域 F 中的元素都是 F 上的代数元.*

证明 对任意 $a\in F$, 只需取 $f(x)=x-a$, 则容易知道 a 是 F 上的代数元. ■

例 6.2.1 $1+\sqrt{2}$ 是代数方程 $(x-1)^2-2=0$ 的根, 故 $1+\sqrt{2}$ 是代数数.

例 6.2.2 1873 年 Hermite 证明了 $\mathrm{e}=2.71828182845904\cdots$ 是超越数, 1882 年 Lindemann 证明了圆周率 π 是超越数.

判断一个数是不是超越数是一件很不容易的事, Gelfond 和 Schneider 在 1934 年独立地证明了 Gelfond-Schneider 定理: 若 α 和 β 都是代数数, $\alpha \neq 0,1$ 并且 β 不是有理数, 则 α^{β} 一定是超越数, 从而解决了 Hilbert 第七问题.

思考题 6.2.1　*若 α 为 F 上的超越元, 则域扩张 $F(\alpha)/F$ 的次数有可能是有限吗?*

不可能. 原因见下面的例子.

例 6.2.3　设 α 为 F 上的超越元, 试证明单扩域 $F(\alpha)$ 是 F 的无限扩域.

证明　反证法. 设 α 是域 F 的超越元, 假设 $F(\alpha)$ 是 F 的 n 次扩域, 则 $F(\alpha)$ 中任意 $n+1$ 个元一定是线性相关的, 因此 $1, \alpha, \alpha^2, \cdots, \alpha^n$ 线性相关, 故存在不全为零的元素 $b_0, b_1, b_2, \cdots, b_n$, 使得

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0.$$

从而 α 是多项式

$$b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n = 0$$

的根, 故 α 是 F 的代数元, 但这与 α 是域 F 的超越元矛盾. 所以, 由反证法原理可知单扩域 $F(\alpha)$ 是 F 的无限扩域. ■

2　极小多项式

定义 6.2.3　*设 K/F 是域扩张, $\alpha \in K$ 是 F 上的代数元, 则有一个次数最低的首一多项式 $f(x) \in F[x]$, 使得 $f(\alpha) = 0$, 这个 $f(x)$ 称为 α 的极小多项式* (minimal polynomial).

例 6.2.4　设 K 是有理数域的扩域, 则 $\sqrt{3}$ 的极小多项式是 $x^2 - 3$.

3　极小多项式的性质

极小多项式是不是唯一的? 它有哪些重要性质呢? 下面定理给出了回答.

定理 6.2.1　*设 K/F 是域扩张, $\alpha \in K$. 若 α 是 F 上的代数元, 其极小多项式是 $f(x)$, 则*

(1) *$f(x)$ 是不可约多项式;*

(2) *若 $g(x) \in F[x]$, 使得 $g(\alpha) = 0$, 则 $f(x)$ 整除 $g(x)$;*

(3) α 的极小多项式是唯一确定的;

(4) $[F(\alpha):F]=\deg(f)$.

证明 (1) 若 $f(x)=g(x)h(x)$, 则 $\deg(g)<\deg(f)$ 且 $\deg(h)<\deg(f)$. 不妨设 $g(x)$ 和 $h(x)$ 都是首一多项式. 由 $f(\alpha)=g(\alpha)h(\alpha)$ 可知, $g(\alpha)=0$ 或 $h(\alpha)=0$, 但这与 $f(x)$ 是 α 的极小多项式矛盾, 所以 $f(x)$ 是不可约多项式.

(2) 不妨设 $g(x)$ 不是零多项式. 由带余除法, 有

$$g(x)=f(x)h(x)+r(x),$$

并且 $\deg(r)<\deg(f)$. 故

$$g(\alpha)=f(\alpha)h(\alpha)+r(\alpha)=r(\alpha)=0.$$

由 $f(x)$ 是 α 的极小多项式可知, $r(x)=0$, 所以 $f(x)$ 整除 $g(x)$.

(3) 设 $g(x)$ 也是 α 的极小多项式, 则 $f(x)$ 整除 $g(x)$, 并且 $g(x)$ 整除 $f(x)$, 由于极小多项式都是首一的, 故 $f(x)$ 等于 $g(x)$, 所以 α 的极小多项式是唯一确定的.

(4) 若 α 是 F 上的代数元, $f(x)$ 是 α 的极小多项式, $n=\deg(f)$, 则不难验证 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 为 $F(\alpha)$ 在 F 的基, 所以 $[F(\alpha):F]=\deg(f)$. ■

4 域的代数扩张

定义 6.2.4 设 K/F 是域扩张, 若 K 中任何元素都是 F 上的代数元, 则称 K/F 为代数扩张 (algebraic extension).

例 6.2.5 由于 $\sqrt{2}$ 是有理数域 $\mathbf{Q}$ 上的代数数, 故 $\mathbf{Q}(\sqrt{2})$ 是 $\mathbf{Q}$ 的代数扩张.

定理 6.2.2 设 K/F 是有限扩张, 则 K 中任何元素都是 F 上的代数元.

证明 设 $[K:F]=n$, 则对任意的 $\alpha\in K$, $1,\alpha,\alpha^2,\cdots,\alpha^n$ 是线性相关的, 因而存在不全为零的 $a_0,a_1,a_2,\cdots,a_n\in F$, 使得

$$a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n=0.$$

所以 α 是 F 上的代数元. ■

由此可见, 若 K/F 是有限扩张, 则 K/F 一定是代数扩张.

思考题 6.2.2 如果 K/F 是代数扩张, 那么 K/F 一定是有限扩张吗?

不一定, 如在有理数域 $\mathbf{Q}$ 上添加所有方程 $x^n-2=0(n=2,3,\cdots)$ 的全体复数根所得到的扩域是代数扩张, 但不是有限扩张.

定理 6.2.3　*域扩张 E/F 是有限扩张当且仅当它是有限生成的代数扩张.*

证明　若 E/F 是有限生成的代数扩张, 则存在代数元 $\alpha_1,\alpha_2,\cdots,\alpha_n\in E$, 使得 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$. 记 $E_i=F(\alpha_1,\alpha_2,\cdots,\alpha_i)$, 则对 $i>1$, E_i 中的元是 E_{i-1} 上的代数元, 故

$$[E_i:E_{i-1}]<\infty,$$

从而

$$[E:F]=[E_n:E_{n-1}]\cdots[E_2:E_1][E_1:F]<\infty.$$

所以域扩张 E/F 是有限扩张.

若 E/F 是有限扩张, 则 E 中任何元素都是 F 上的代数元, 故 E/F 是代数扩张. 令 $\beta_1,\beta_2,\cdots,\beta_n$ 是域 F 的向量空间 E 的一组基, 则 $E=F(\beta_1,\beta_2,\cdots,\beta_n)$, 所以 E/F 是有限生成的代数扩张. ■

Brandis 在 1965 年证明了若 F 是无限域, 则对 F 的任意真扩张 E, 商群 E^*/F^* 不是有限生成的, 这里 E^* 和 F^* 分别是 E 和 F 的乘法群①.

5　代数扩张的传递性

容易知道, 若 E/F 和 L/E 都是有限扩张, 则 L/F 是有限扩张, 因此可以考虑下面问题.

思考题 6.2.3　*若 E/F 和 L/E 都是代数扩张, 则 L/F 是代数扩张吗?*

设 K 是扩张 E/F 的中间域, $\alpha\in E$ 是 F 上的代数元, 根据代数元定义, 存在系数在 F 中的非零多项式 $f(x)$, 使 $f(\alpha)=0$. 既然 K 包含 F, $f(x)$ 也是一个系数在 K 中的非零多项式, 所以 α 也是 K 上的代数元. 代数扩张具有如下的传递性.

定理 6.2.4　*设 E/F 和 L/E 都是代数扩张, 则 L/F 是代数扩张.*

证明　对任意的 $\alpha\in L$, 由于 α 是 E 上的代数元, 故存在极小多项式 $f(x)$, 使得 $f(\alpha)=0$.

① Brandis A. Über die multiplikative Struktur von Körpererweiterungen. Math. Z., 1965, 87: 71–73.

极小多项式 $f(x)$ 是首 1 多项式, 故可以设

$$f(x)=b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1}+x^n,$$

其中 $b_0,b_1,b_2,\cdots,b_{n-1}\in E$.

由 $b_0,b_1,b_2,\cdots,b_{n-1}$ 都是 F 上的代数元可知, $F(b_0,b_1,b_2,\cdots,b_{n-1})$ 是 F 的有限扩张.

由于 $f(\alpha)=0$, α 是 $F(b_0,b_1,b_2,\cdots,b_{n-1})$ 上的代数元, 故

$$[F(b_0,b_1,b_2,\cdots,b_{n-1},\alpha):F(b_0,b_1,b_2,\cdots,b_{n-1})]<\infty.$$

由 $[F(b_0,b_1,b_2,\cdots,b_{n-1}):F]<\infty$ 和域扩张的次数公式可知

$$[F(b_0,b_1,b_2,\cdots,b_{n-1},\alpha):F]<\infty,$$

所以, α 是 F 上的代数元. ■

6 代数闭域

Steinitz 引进了代数闭域, 在 1910 年证明了对任意域 F, 都存在唯一的代数扩张 K 是代数闭域.

定义 6.2.5 *设 K 是一个域, 若 K 上的每个非常数的多项式在 K 上有根, 则称 K 是一个代数闭域* (algebraically closed field).

由于多项式 x^2-2 在有理数域 $\mathbf{Q}$ 上没有根, 故有理数域 $\mathbf{Q}$ 不是一个代数闭域. 多项式 x^2+1 在实数域 $\mathbf{R}$ 上没有根, 因此有实数域 $\mathbf{R}$ 也不是一个代数闭域.

例 6.2.6 由代数基本定理可知, 任何一个复系数多项式都至少有一个复数根, 因此复数全体 $\mathbf{C}$ 是一个代数闭域.

下面给出代数闭域的一些性质.

定理 6.2.5 *设 K 是一个域, 则下列命题等价:*

(1) *K 是代数闭域;*

(2) *K 上的任意一个非常数的多项式 $f(x)$ 都有一次因子;*

(3) *K 上的任意一个非常数的多项式 $f(x)$ 都可以分解成一次因子的乘积, 即 $f(x)=a(x-a_1)(x-a_2)\cdots(x-a_n)$ 对 $a_i\in K$, 但 a_i 不一定互不相同.*

证明　(1)⇒(2) 若 K 是代数闭域, 非常数的多项式 $f(x) \in K[x]$, 则 $f(x)$ 在 K 有根 a, 因此 $x-a$ 是 $f(x)$ 的一次因子.

(2)⇒(3) 非常数的多项式 $f(x) \in K[x]$, 则 $f(x)$ 在 K 有一次因子 $x-a_1$, 因此 $f(x)=(x-a_1)g_1(x)$, 若 $g_1(x)$ 的次数大于 1, 则 $g_1(x)$ 在 K 也有一次因子 $x-a_2$, 使得 $g_1(x)=(x-a_2)g_2(x)$, 因此 $f(x)=(x-a_1)(x-a_2)g_2(x)$. 从而容易知道 $f(x)$ 可以分解成一次因子的乘积.

(3)⇒(1) 这是明显的. ■

思考题 6.2.4　*代数闭域是否可能是有限域?*

不可能. 若域 F 是有限域, 并且只有 q 个元素, 则 q 次多项式 $f(x)=\Pi_{a\in F}(x-a)+1$ 在 F 上没有根, 因此 F 不是代数闭域, 所以代数闭域一定是无限域.

Shipman 在 2007 年证明了若域 F 上的每个素数次多项式在 F 上有根, 则 F 一定是代数闭域①.

6.3　Galois 域和分裂域

有理数域、实数域等常见的域含有无限多个元素, p 为素数时, 域 $\mathbf{Z}_p$ 只含有限个元素. 有限域指的是元素个数有限的域, 有限域的结构比较容易掌握, 它有许多独特的性质, 有限域在组合数学、有限几何、编码理论中有很多应用.1830 年, Galois 发表了一篇重要的论文论数论 (Sur la Theorie des Nombres). Galois 采用域扩张的方法, 构造出所有可能的有限域. 证明每个有限域的元素个数必为某个素数 p 方幂 p^n, 并且对每个素数幂 p^n, 本质上只有一个 p^n 个元的有限域. 因此, 后来就将有限域称为 Galois 域.

1　Galois 域的定义

定义 6.3.1　*元素个数有限的域称为有限域或 Galois 域.*

例 6.3.1　当 p 为素数时, $\mathbf{Z}_p$ 为 Galois 域, 它的特征为 p.

容易知道可除环不一定是域, 如四元数可除环就是最简单的非交换可除环, 但它不是域. Wedderburn 在 1905 年证明了任意有限可除环一定是可交换环, 因此有

① Shipman J. Improving the fundamental theorem of algebra. Math. Intelligencer, 2007, 29(4): 9–14.

限可除环一定是域.

2 Galois 域的元素个数

定理 6.3.1 设有限域 F 的特征为 p, F 的素子域为 F_0, $[F:F_0]=n$, 则有限域 F 中元素个数为 p^n.

证明 由于有限域 F 的特征为 p, 故 F 含有素子域 $F_0\cong \mathbf{Z}_p$, 故 $|F_0|=p$. 由 F 是 F_0 上的向量空间和 $[F:F_0]=n$ 可知, F 中每个元素都可以唯一地表示为

$$a_1u_1+a_2u_2+\cdots+a_nu_n,$$

其中 $a_1,a_2,\cdots,a_n\in F_0$, $u_1,u_2,\cdots,u_n$ 是 F 在 F_0 的一组基, 由于每个 a_i 可以取 F_0 中 p 个不同的元素, 同时 $u_1,u_2,\cdots,u_n$ 线性无关, 所以 F 含有 p^n 个不同的元素. ■

3 多项式的分裂域的定义

在有理数域 $\mathbf{Q}$ 上, 多项式 $f(x)=x^2+1$ 不能分解为一次因子的乘积, 但可以找到 $\mathbf{Q}$ 的一个代数扩域 $\mathbf{Q}(\mathrm{i})$, 使得在 $\mathbf{Q}(\mathrm{i})$ 上 $f(x)=x^2+1$ 可以分解为一次因子的乘积, 因此考虑下面的问题是很自然的.

思考题 6.3.1 对于给定的域 F 和 $F[x]$ 中的多项式 $f(x)$, 是不是一定存在 F 的扩域 K, 使得 $f(x)$ 在 $K[x]$ 中能够分解成一次因式的乘积呢?

定义 6.3.2 设 F 为域, $f(x)$ 为 F 上的首 1 多项式, E 为 F 的扩域, 若

(1) $E=F(a_1,a_2,\cdots,a_n)$;

(2) $f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)$.

则 E 称为 $f(x)$ 在 F 上的分裂域 (splitting field) 或根域 (root field).

分裂的意思是指 $f(x)$ 能在这个域中分解成一次因子的乘积. 对于给定的 $f(x)\in F[x]$, 它的根 $a_1,a_2,\cdots,a_n$ 都是 F 上代数元, 把它们加到域 F 上, 就可得到 F 的有限添加代数元扩域 $E=F(a_1,a_2,\cdots,a_n)$, 它是 F 的有限扩域, 容易知道域 E 就是 $f(x)$ 在 F 上的分裂域, 因此, 有时候也将分裂域称为根域.

例 6.3.2 $\mathbf{Q}(\sqrt{2})$ 为 $f(x)=x^2-2$ 在 $\mathbf{Q}$ 的分裂域.

4　多项式的分裂域的存在性和唯一性

定理 6.3.2 (Kronecker 定理)　*设 F 为域, $f(x)$ 是 $F[x]$ 中的一个不是常数的多项式, 则一定存在 F 的一个扩域 K, 包含 $f(x)$ 的一个根.*

证明　(1) 若多项式 $f(x)$ 的次数为 1, 只需取 $K=F$, 则 $f(x)$ 在 K 上有一个根.

(2) 若多项式 $f(x)$ 的次数大于 1, 由于多项式环 $F[x]$ 是唯一分解整环, 故存在不可约多项式 $p(x)$, 使得 $f(x)=p(x)g(x)$.

(3) 下面的证明主要是构造 F 的一个扩域, 使得 $p(x)$ 在该扩域上有一个根.

① 用 $(p(x))$ 记 $p(x)$ 生成的理想, 由于 $p(x)$ 是不可约多项式, 故商环 $F[x]/(p(x))$ 是一个域.

② 容易验证映射

$$\varphi : F \to F[x]/(p(x)),$$

$$\varphi(a) = a + (p(x))$$

是 F 到 $F[x]/(p(x))$ 的子域 $F'=\{a+(p(x))|a\in F\}$ 的同构.

③ 由 φ 可诱导出 $F[x]$ 到 $F'[x]$ 的一个同构 $\overline{\varphi}$

$$\overline{\varphi} : F[x] \to F'[x],$$

$$\begin{aligned}&\overline{\varphi}(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0)\\ &= \varphi(a_n)x^n + \varphi(a_{n-1})x^{n-1} + \cdots + \varphi(a_1)x + \varphi(a_0).\end{aligned}$$

此时, 将 $\overline{\varphi}(f(x))$ 记为 $\overline{f}(x)$.

④ 设 $p(x)$ 的形式为

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad (\text{这里} a_i \in F).$$

则

$$\begin{aligned}\overline{p}(x) = &(1+(p(x)))x^n + (a_{n-1}+(p(x)))x^{n-1}\\ &+ \cdots + (a_1+(p(x)))x + (a_0+(p(x))).\end{aligned}$$

令 $\alpha = x+(p(x))$, 则 $\alpha \in F[x]/(p(x))$. 下面证明 α 是 $\overline{p}(x)$ 的根.

将 $\alpha = x + (p(x))$ 代入上面 $\overline{p}(x)$ 的表达式, 得

$$\begin{aligned}\overline{p}(\alpha) &= (1+(p(x)))(x+(p(x)))^n + (a_{n-1}+(p(x)))(x+(p(x)))^{n-1} \\ &\quad + \cdots + (a_1+(p(x)))(x+(p(x))) + (a_0+(p(x))) \\ &= (1+(p(x)))(x^n+(p(x))) + (a_{n-1}+(p(x)))(x^{n-1}+(p(x))) \\ &\quad + \cdots + (a_1+(p(x)))(x+(p(x))) + (a_0+(p(x))) \\ &= (x^n+(p(x))) + (a_{n-1}x^{n-1}+(p(x))) + \cdots + (a_1x+(p(x))) + (a_0+(p(x))) \\ &= x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 + (p(x)) \\ &= p(x) + (p(x)) = (p(x)).\end{aligned}$$

由于 $(p(x)) = 0 + (p(x))$ 是 $F[x]/(p(x))$ 的零元, 故由 $\overline{p}(\alpha) = 0$ 可知, α 为 $\overline{p}(x)$ 在 $F[x]/(p(x))$ 的根.

⑤ 由于域 F 与域 F' 是同构的, 故一般将它们看做是一样的, 因而 $F[x]/(p(x))$ 可看做 F 的扩域, 并且 $p(x)$ 在该扩域上有一个根, 所以 $f(x)$ 在该扩域上有一个根.

例 6.3.3 在实数域 $\mathbf{R}$ 上, $f(x) = x^2+1$ 在 $\mathbf{R}$ 上没有根, 由于 x^2+1 是不可约多项式, 因此 $K = \mathbf{R}[x]/(f(x))$ 可以看做是 $\mathbf{R}$ 的域扩张, 并且对于 $i = x+(f(x))$, 有

$$\overline{f}(x) = (1+(f(x)))x^2 + (1+(f(x))).$$

故

$$\begin{aligned}\overline{f}(i) &= (1+(f(x)))(x+(f(x)))^2 + (1+(f(x))) \\ &= (x^2+(f(x))) + (1+(f(x))) \\ &= 1 + x^2 + (f(x)) = (f(x)) = 0.\end{aligned}$$

因此多项式 x^2+1 在扩域 K 上有根.

Kronecker 定理是域论中最基本的结果之一. 利用上面定理, 可以证明对 F 上任意的多项式 $f(x)$, $f(x)$ 在 F 上的分裂域一定存在.

定理 6.3.3 *设 F 为域, $f(x) \in F[x]$, $f(x)$ 在 F 上的分裂域 E 一定存在.*

证明 依 $f(x)$ 的次数 n, 用数学归纳法来证明.

(1) 当 $n = 1$ 时, 若 $\deg(f) = 1$, 取 $E = F$, 则 E 就是 $f(x)$ 在 F 上的分裂域.

(2) 假设对于 $\deg(f) < n$ 时, 结论成立.

(3) 下面证明 $\deg(f)=n$ 时, 结论成立.

若 $f(x)$ 在 F 上是可约多项式, 则存在次数小于 n 的多项式 $g(x)$ 和 $h(x)$, 使得 $f(x)=g(x)h(x)$.

由归纳假设知, 存在 $g(x)$ 在 F 上的分裂域 E_1, 包含 $g(x)$ 的所有根 $a_1,a_2,\cdots,a_m$. 将 $h(x)$ 看做 $F(a_1,a_2,\cdots,a_m)$ 上的多项式, $h(x)$ 是次数小于 n 的多项式, 故存在 $h(x)$ 在 $F(a_1,a_2,\cdots,a_m)$ 上的分裂域 E, E 包含 $h(x)$ 的所有根. 从而 E 含有 $f(x)$ 的所有根, 所以 E 是 $f(x)$ 在 F 上的分裂域.

若 $f(x)$ 在 F 上是不可约多项式, 由 Kronecker 定理, 存在 F 的扩域 K, 使得 K 含有 $f(x)$ 的一个根 β. 于是在 $K[x]$ 中, $f(x)=(x-\beta)u(x)$.

由于 $u(x)$ 的次数为小于 n, 由归纳假设可知, 一定存在 K 上的分裂域 E, 含有 $u(x)$ 的所有根, 从而 E 也含有 $f(x)$ 的所有根, 所以 E 是 $f(x)$ 在 F 上的分裂域. ■

对于有限域的分裂域, 有下面的结论成立.

定理 6.3.4　*设有限域 F 的特征为 p, F 的素子域为 F_0, F 含有 p^n 个元素, 则 F 是多项式 $x^{p^n}-x$ 在 F_0 的分裂域.*

证明　由于 $F^*=F\backslash\{0\}$ 对于乘法是一个 p^n-1 阶的群, 故对任意的 $a\in F^*$, 有 $a^{p^n-1}-1=0$, 所以对任意的 $a\in F$, 都有 $a^{p^n}-a=0$, 因而若用 $a_1,a_2,\cdots,a_{p^n}$ 来表示 F 的元, 则在 F 中, 有

$$x^{p^n}-x=(x-a_1)(x-a_2)\cdots(x-a_{p^n}).$$

故 $F_0[x]$ 中的多项式 $x^{p^n}-x$ 在 F 中有 p^n 个不同的根. 因此 $F=F_0(a_1,a_2,\cdots,a_{p^n})$, 所以 F 是多项式 $x^{p^n}-x$ 在 F_0 的分裂域. ■

若 F 是有限域, 则 F 的元素个数一定是某个素数 p 的幂, 那反过来呢?

思考题 6.3.2　*对任意的素数 p 的幂 p^n, 是否一定存在有限域, 它的元素个数为 p^n?*

是的. Galois 证明了若 p 是素数, n 是正整数, 则存在恰好有 p^n 个元素的域.

定理 6.3.5　*若 p 是素数, $n\in\mathbf{Z}$, $n\geqslant 1$, 则多项式 $x^{p^n}-x$ 在 $\mathbf{Z}_p$ 的分裂域是一个恰好有 p^n 个元素的域.*

证明　(1) 先证明多项式 $x^{p^n}-x$ 有 p^n 个不同的根.

设 $a_1, a_2, \cdots, a_{p^n}$ 为 $f(x) = x^{p^n} - x$ 的根, 由于 $\mathbf{Z}_p$ 的特征为 p, 故 $f(x) = x^{p^n} - x$ 的导数为 $f'(x) = p^n x^{p^n-1} - 1 = -1$, 于是 $(f(x), f'(x)) = 1$, 因此 $x^{p^n} - x$ 没有重根, 因而 $f(x) = x^{p^n} - x$ 有 p^n 个不同的根.

(2) 下面证明 $f(x)$ 的根构成一个加法群.

若 a_1, a_2 是 $f(x)$ 的根, 则

$$(a_1 - a_2)^{p^n} - (a_1 - a_2) = a_1^{p^n} - a_2^{p^n} - a_1 - a_2 = 0.$$

故 $a_1 - a_2$ 是 $f(x)$ 的根, 因此 $f(x)$ 的根构成一个加法群.

(3) 再证明 $f(x)$ 的根构成一个乘法群.

若 a_1, a_2 是 $f(x)$ 的根, 则

$$(a_1 a_2)^{p^n} - (a_1 a_2) = 0.$$

因此 $a_1 a_2$ 都是 $f(x)$ 的根.

另外, 若 a 是 $f(x)$ 的非零根, 则 $a^{p^n} = a$, 故

$$(a^{-1})^{p^n} - a^{-1} = (a^{p^n})^{-1} - a^{-1} = 0.$$

因此 a^{-1} 是 $f(x)$ 的根, 从而 $f(x)$ 的根构成一个乘法群.

(4) 由 (2) 和 (3) 可知, $f(x)$ 的根全体 $\{a_1, a_2, \cdots, a_{p^n}\}$ 是一个域.

(5) 由于对任意 $a \in \mathbf{Z}_p$ 都有 $a^{p^n} - a = 0$, 故 $\mathbf{Z}_p \subseteq \{a_1, a_2, \cdots, a_{p^n}\}$. 由分裂域的定义可知, $\{a_1, a_2, \cdots, a_{p^n}\}$ 是 $x^{p^n} - x$ 在 $\mathbf{Z}_p$ 上的分裂域, 并且恰好有 p^n 个元素的域. ■

同阶有限群或环不一定同构, 但元素一样多的有限域却是同构的. 或者说, 有限域的性质是由其所含元素的个数唯一决定.

命题 6.3.1 *同样多个元素的域一定是同构的.*

证明 若域 E 和 F 的元素个数相等, 则由于有限域的特征一定是某个素数 p, 元素个数必为某个素数 p 的幂, 故不妨记为 p^n, 则 E 和 F 的素子域都与 $\mathbf{Z}_p$ 同构, 并且 E 和 F 都是它们的素子域上多项式 $x^{p^n} - x$ 的分裂域, 所以 E 和 F 是同构的. ■

5　Galois 域是其素子域的单扩域

Galois 域有一个重要的性质, 即 Galois 域 F 是其素子域 E 的单扩域. 为证明该结论, 先看看有限交换群的一个结论.

引理 6.3.1　*若 G 为有限交换群, m 为 G 中元素的阶的最大者, 则 m 能被 G 的每个元素的阶整除.*

证明　反证法. 假设 G 中元素 b 的阶为 n, 但 n 不能整除 m, 则存在素数 p, 满足

$$m = m_1 p^s, \quad n = n_1 p^t, \quad s < t, \quad (p, m_1) = 1.$$

设 G 中元素 a 的阶为 m, 取

$$a_1 = a^{p^s}, \quad b_1 = b^{n_1},$$

则 a_1 的阶为 m_1, b_1 的阶为 p^t, 并且 $(p^t, m_1) = 1$, 由于 G 是交换群, 故 $a_1 b_1$ 的阶为 $m_1 p^t$, 并且 $m_1 p^t > m$, 但这与 m 为 G 中元素的阶的最大者矛盾, 所以由反证法原理可知, m 能被 G 的每个元素的阶整除. ■

有限域中有两个交换群, 一个是域的加法群, 一个是所有非零元构成的乘法群. 有限域 F 的乘法群 $F^* = F\backslash\{0\}$ 实际上是循环群. 由上面引理可以得到 Galois 域的一个重要刻画.

定理 6.3.6　*Galois 域是其素子域的单扩域.*

证明　(1) 设 Galois 域 F 的阶为 p^n, F_0 为它的素子域, 则 $F^* = F\backslash\{0\}$ 对乘法是一个阶为 $p^n - 1$ 的交换群.

(2) 下面证明 F^* 是 a 生成的循环群.

若 a 为 F^* 中阶最大的元素, a 的阶为 m, 则由上面引理可知, 对于 F^* 的任意元素 b, m 能被 b 的阶整除, 故一定有 $b^m = 1$, 因此 F^* 中每个元素都是 $x^m - 1$ 的根. 因而 $x^m - 1$ 至少有 $p^n - 1$ 个根, 故多项式 $x^m - 1$ 的次数至少是 $p^n - 1$, 即 $m \geqslant p^n - 1$. 由于 F^* 的阶为 $p^n - 1$, a 为 F^* 中的元素, 故由 Lagrange 定理可知 m 整除 $|F^*|$, 因而 $m \leqslant p^n - 1$, 故 $m = p^n - 1$, 因而 F^* 是 a 生成的循环群.

(3) 由 $a \in F^* \subseteq F$ 和 $F_0 \subseteq F$ 可知, $F_0(a) \subseteq F$, 即域 F 包含它的素子域 F_0 添加 a 得到的单扩域 $F_0(a)$. 另外, 由于 $F^* = < a >, F = F^* \cup \{0\}$, 故 $F \subseteq F_0(a)$. 所以, Galois 域是其素子域 F_0 的单扩域 $F_0(a)$. ■

例 6.3.4 试作出含 8 个和 32 个元素的域.

证明 多项式 x^8-x 在 $\mathbf{Z}_2$ 的分裂域 E 含 8 个元素, 多项式 $x^{32}-x$ 在 $\mathbf{Z}_2$ 的分裂域 F 含 32 个元素. ■

例 6.3.5 试证明没有含 200 个元素的域.

证明 因为 $200=2^3\cdot 5^2$, 它不是某个素数的幂, 所以没有恰好含 200 个元素的域. ■

6 正规扩域

$f(x)$ 的分裂域与 $f(x)$ 的系数所在的域 F 有关, 多项式的分裂域具有某种正规性.

定义 6.3.3 *设 E 是 F 的代数扩域, 如果 E 满足以下条件: $F[x]$ 中的任一不可约多项式 $f(x)$, 或者在 E 中无根, 或者每个根都在 E 中, 则称 E 是 F 的正规扩域或正规扩张* (normal extension).

容易知道, 由于不可约多项式 $f(x)=x^2-2$ 在 $\mathbf{Q}(\sqrt{2})$ 中有根, 并且 $f(x)$ 的根都在 $\mathbf{Q}(\sqrt{2})$ 中, 故容易证明 $\mathbf{Q}(\sqrt{2})$ 是 $\mathbf{Q}$ 的正规扩张. 由于不可约多项式 $f(x)=x^3-2$ 在 $\mathbf{Q}(\sqrt[3]{2})$ 中有根, 但 $f(x)$ 的根有的不在 $\mathbf{Q}(\sqrt[3]{2})$ 中, 故 $\mathbf{Q}(\sqrt[3]{2})$ 不是 $\mathbf{Q}$ 的正规扩张. 对于正规扩张, 可以证明下面的结论成立.

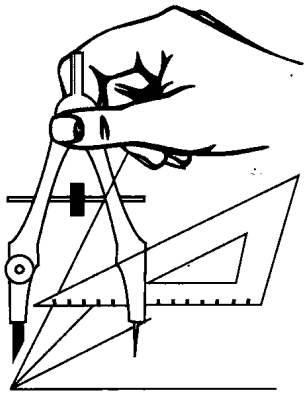
定理 6.3.7 (1) *设 E 是 F 的扩张, 则 E 是 F 的正规扩张的充要条件为 E 是 $F[x]$ 的一族多项式的分裂域.*

(2) *设 E 是 F 的有限扩张, 则 E 是 F 的正规扩张的充要条件为 E 是 $F[x]$ 的某个多项式 $f(x)$ 的分裂域.*

7 圆规和直尺作图

用圆规和直尺作图是中学几何的内容之一, 下面来研究尺规作图问题. 并证明几何三大问题不可能用圆规和直尺作出.

尺规作图所使用的直尺不带刻度, 过两点可以画一条直线. 圆规两脚可以任意张开, 以一点为圆心, 以定长为半径可以画圆截取定长. 所谓尺规作图, 就是在平面上给定一些初等几何图形, 点、线、圆, 利用这些图形, 来作一些满足特定要求的几何图形, 但在作图的过程中, 只能用圆规和直尺. 一个几何图形可以用平面上的有



限个点来代表.

定义 6.3.4　实数 a 称为可用尺规作出的, 若它可以从整数坐标点出发, 通过有限次的圆规直尺作图构作出来.

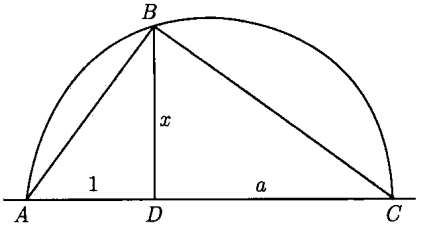
明显地, a 可用尺规作出等价于长为 $|a|$ 的直线可用尺规作出. 先看看下面的几个用尺规作图的例子.

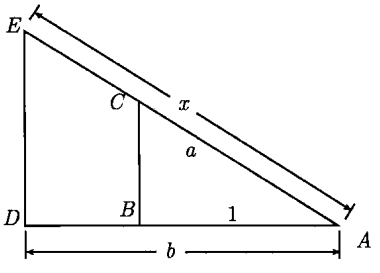
例 6.3.6　若 a 是可用尺规作出的, 试用尺规作出 $\sqrt{a}$.

解　如果 a 是可用尺规作出的, 则用尺规可以作出左下图, 容易知道三角形 ABD 和三角形 BCD 是相似的, 则 $\dfrac{AD}{BD}=\dfrac{BD}{DC}$, 故 $\dfrac{1}{x}=\dfrac{x}{a}$, 因此 $x^2=a$, 从而 $\sqrt{a}$ 是可用尺规作出的. ■

例 6.3.7　若 a 和 b 可用尺规作出的, 试用尺规作出 ab.

解　如果 a 和 b 是可用尺规作出的, 则用尺规可以作出右下图, 容易知道三角形 ABC 和三角形 ADE 是相似的, 则 $\dfrac{AB}{AD}=\dfrac{AC}{AE}$, 故 $\dfrac{1}{b}=\dfrac{a}{x}$, 因此 $x=ab$, 从而 ab 是可用尺规作出的.





按上面例子的方法, 整数显然是可用尺规作出的, 不难知道下列结论成立:

(1) 每个有理数均是可用尺规作出的;

(2) 如果 $a>0$ 是可用尺规作出的, 则 $\sqrt{a}$ 也是可用尺规作出的;

(3) 如果 a 和 b 是可用尺规作出的, 则 $a\pm b$, ab 和 $\dfrac{b}{a}(a\neq 0)$ 都是可用尺规作

出的, 全体可用尺规作出的实数构成实数域的一个子域, 并且它包含有理数域.

思考题 6.3.3 *若实数 a 可用尺规作出, 则 a 具有什么特点呢?*

容易理解, 若实数 a 可用尺规作出, 则 a 一定是下面三种情况之一:

(1) a 为两条直线的交点, 因此它是两个直线方程的公共解.

$$\begin{cases} a_1x + b_1y = c_1, \\ a_2x + b_2y = c_2. \end{cases}$$

(2) a 为一条直线和一个圆的交点, 因此它是直线方程与圆方程的公共解.

$$\begin{cases} a_1x + b_1y = c_1, \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0. \end{cases}$$

(3) a 为两个圆的交点, 因此它是两个圆方程的公共解.

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0, \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0. \end{cases}$$

将 (3) 中的两个方程相减可知, a 可看做一条直线和一个圆的交点, 因此只需考虑如下方程.

$$\begin{cases} y = kx + b, \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0. \end{cases}$$

将 $y = kx + b$ 代入 $x^2 + y^2 + a_2x + b_2y + c_2 = 0$ 后, 得到 $d_2x^2 + d_1x + d_0 = 0$, 因而关于尺规作图, 可以进一步证明下面定理成立.

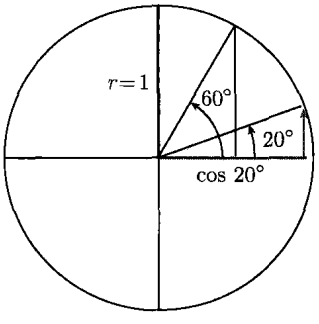
定理 6.3.8 *若实数 a 可用尺规作出, 则 a 必是有理数域 $\mathbf{Q}$ 上的代数元, 并且其极小多项式的次数等于 2 的幂.*

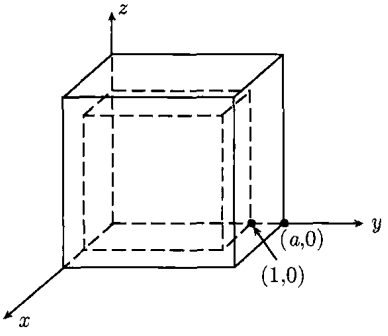
下面来讨论几个著名的作图问题, 在这几个问题中只需已知两个点. Wantzel 在 1837 年证明不能用尺规三等分任意一个角和不能用尺规将立方体的体积倍增①.

例 6.3.8 试证明不能用尺规三等分任意一个角.

证明 明显地, 只需证明 60° 角不可能用尺规三等分就可以了.

① Wantzel P L. Recherches sur les moyens de reconnaître si un probléme de Géométrie peut se résoudre avec la règle et le compass. Journal de Mathématiques Pures et Appliquées, 1837, 1(2): 366–372.





反证法. 假设 60° 角可以用尺规三等分, 则 20° 角可以用尺规作出, 因而 $\cos 20°$ 也可以用尺规作出. 由三倍角公式

$$\cos 60° = 4\cos^3 20° - 3\cos 20°$$

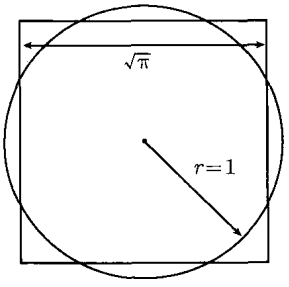
可知, $a = \cos 20°$ 是方程 $4x^3 - 3x - \dfrac{1}{2} = 0$ 的根. 容易验证 $x^3 - \dfrac{3}{4}x - \dfrac{1}{8} = 0$ 无有理根, 故多项式

$$f(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$$

是 $\mathbf{Q}$ 上的不可约多项式, 而 $f(x)$ 是一个三次多项式, 于是 $f(x)$ 是 a 的极小多项式, 它的次数等于 3. 与定理 6.3.8 矛盾, 由反证法原理可知 60° 角不可能用尺规三等分. ■

例 6.3.9　试证明不能用尺规将立方体的体积倍增.

证明　要作出正方体使的它的体积是已知正方体的 2 倍, 如果设已知正方体边长为 1, 则所求的立方体的体积为 2, 因此所求的立方体的边长为 $\sqrt[3]{2}$. 由于 $\sqrt[3]{2}$ 是 $x^3 - 2 = 0$ 的根, 并且在 $f(x) = x^3 - 2$ 上 $\mathbf{Q}$ 不可约, 故 $\sqrt[3]{2}$ 在 $\mathbf{Q}$ 上的极小多项式为 $f(x) = x^3 - 2$, 它的次数等于 3, 不是 2 的幂, 所以它不能用尺规作出. ■



Lindemann 在 1882 年证明了 π 是超越数, 从而用尺规作出一个正方形使它的面积等于一个已知圆的面积是不可能的.

例 6.3.10　试证明不能用尺规作出一个正方形使它的面积等于一个已知圆的面积.

证明　设已知圆的半径为 1, 则要作出面积等于 π 的正方形, 因此所求的正方形的边长为 $\sqrt{\pi}$, 但 π 是一个超越数, 由于任一代数数的平方还是代数数, 故 $\sqrt{\pi}$ 也是超越数, 所以它不能用尺规作出. ■

6.4 方程的根式解

对一元一次方程 $ax+b=0$ 及一元二次方程 $ax^2+bx+c=0$, 它们都可以用根式求解:

$$x=-\frac{b}{a},\quad x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

对于一元三次方程及一元四次方程, 也可以用根式求解. 对于一个一元 n 次方程 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$, 根据代数基本定理, 根总是存在的, 但是否有根式解呢? 所谓根式解, 就是经过有限次的加、减、乘、除和开方运算, 把一个一元 n 次方程的根求出来. 人们原以为对五次及五次以上方程也可以用根式求解, 但经过长达几百年的努力, 这种努力都归于失败. 挪威数学家 Abel 在 1824 年证明了一般五次方程根式解的不可能性.1830 年前后, 法国数学家 Galois 借助于由他创立的群的理论彻底地解决了这个问题, Galois 的工作非常漂亮地解决了一元 n 次方程的求根问题.

1 Galois 群

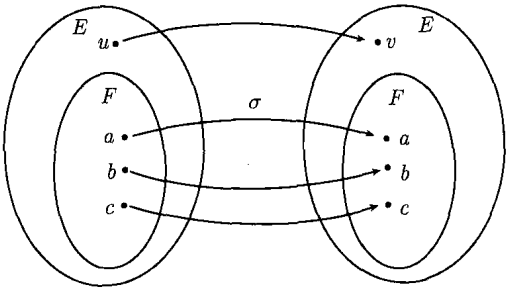
一个域到自身的同构称为**自同构**, 由于群的自同构必把单位元变为单位元, 故域的自同构必把 $(E,+)$ 的单位元 0 变为 0, $(E^*,\cdot)$ 的单位元 1 变为 1.E 的自同构全体关于变换复合构成群, 称为 E 的**自同构群**, 记为 Aut E.

定义 6.4.1 *若 E 是 F 的扩域, 则自同构集合*

$$\mathrm{Gal}(E/F)=\{\sigma|\sigma\in \mathrm{Aut}\ E,\sigma(a)=a \text{ 对任意 } a\in F \text{ 成立}\}$$

是 Aut E 的子群, 称为 E/F 的 Galois 群.

如下图所示, Galois 群 $\mathrm{Gal}(E/F)$ 保持 F 中的元素不变.



例 6.4.1　对域扩张 $\mathbf{C}/\mathbf{R}$, 这里 $\mathbf{R}$, $\mathbf{C}$ 分别为实数域和复数域, 试求 $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$.

证明　任取 $\sigma \in \mathrm{Gal}(\mathbf{C}/\mathbf{R})$, 则对任意实数 a, 都有 $\sigma(a) = a$.

设 $\sigma(\mathrm{i}) = a + b\mathrm{i}$, $a, b \in \mathbf{R}$, 则

$$\sigma(\mathrm{i}^2) = (a + b\mathrm{i})^2 = a^2 - b^2 + 2ab\mathrm{i}$$

由于 $\sigma(-1) = -1$, 故 $a^2 - b^2 = -1$, $2ab = 0$, 由此得 $a = 0, b = \pm 1$. 故

$$\sigma(\mathrm{i}) = \mathrm{i} \quad 或 \quad \sigma(\mathrm{i}) = -\mathrm{i}.$$

因此, $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ 是一个 2 阶循环群. ■

例 6.4.2　设 $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ 为有理数 $\mathbf{Q}$ 上的扩张, 试求 $\mathrm{Gal}(\mathbf{Q}(\sqrt{3}, \sqrt{5})/\mathbf{Q})$.

解　容易知道, 对于 $\mathbf{Q}(\sqrt{3}, \sqrt{5})/\mathbf{Q}$ 的 Galois 群中的元素 τ, 都有

$$\tau(\sqrt{3})^2 = \tau(3) = 3,$$

$$\tau(\sqrt{5})^2 = \tau(5) = 5.$$

因此一定有 $\tau(\sqrt{3}) = \pm\sqrt{3}$ 和 $\tau(\sqrt{5}) = \pm\sqrt{5}$.

故 $\mathrm{Gal}(\mathbf{Q}(\sqrt{3}, \sqrt{5})/\mathbf{Q})$ 中的同构只能是下面几种:

$$\tau : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{5} \mapsto \sqrt{5},$$

$$\sigma : \sqrt{3} \mapsto \sqrt{3}, \sqrt{5} \mapsto -\sqrt{5}$$

和

$$\mu = \tau\sigma : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{5} \mapsto -\sqrt{5}.$$

因此 σ, τ, μ 构成的 Galois 群为 $\mathrm{Gal}(\mathbf{Q}(\sqrt{3}, \sqrt{5})/\mathbf{Q}) = \{e, \sigma, \tau, \mu\}$, 并且有下面的群表.

$\cdot$	e	σ	τ	μ
e	e	σ	τ	μ
σ	σ	e	μ	τ
τ	τ	μ	e	σ
μ	μ	τ	σ	e

所以, $\mathrm{Gal}(\mathbf{Q}(\sqrt{3}, \sqrt{5})/\mathbf{Q})$ 与 $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ 同构. ■

定义 6.4.2 设 F 是任一域, $f(x) \in F[x]$, $f(x)$ 在 F 上的分裂域是 E, 则称 $\mathrm{Gal}(E/F)$ 为 $f(x)$ 在 F 上的 Galois 群, 并记为 G_f.

例 6.4.3 设 $f(x) = x^3 + x + \bar{1}$ 为 $\mathbf{Z}_2$ 上的多项式, 试求 f 的 Galois 群.

解 设 a 为 $f(x)$ 的一个根, 则 $a, a^2, a^2 + a$ 是 $f(x)$ 两两不同的根. 由 $f(\bar{0}) = \bar{1}$ 和 $f(\bar{1}) = \bar{1}$ 可知 $a \notin \mathbf{Z}_2$, 并且 $f(x)$ 在 $\mathbf{Z}_2$ 上是不可约的, 因此 $|G_f| = [\mathbf{Z}_2(a) : \mathbf{Z}_2] = 3$, 因为 S_3 的三阶子群是 A_3, 所以 $G_f = A_3$. ■

2 Galois 群的性质

由某个多项式 $f(x)$ 确定的 Galois 群有一个重要的性质.

性质 6.4.1 设 F 是任一域, $f(x) \in F[x]$, E 为 $f(x)$ 在 F 上的分裂域, G_f 为 $f(x)$ 在 F 上的 Galois 群, 则任意 $\sigma \in G_f$ 都将 $f(x)$ 的根映为 $f(x)$ 的根.

证明 设

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

任取 $f(x)$ 的一个根 a, $a \in E$, 且

$$a_0 + a_1 a + \cdots + a_n a^n = 0.$$

任取 $\sigma \in G_f$, 由于 σ 是域的自同构, 且不改变 $f(x)$ 所有的系数, 故

$$a_0 + a_1 \sigma(a) + \cdots + a_n \sigma(a)^n = 0.$$

从而 $\sigma(a)$ 也是 $f(x)$ 的根. ■

定义 6.4.3 设 H 是 $\mathrm{Aut}\ E$ 的一个子群, 令 $\mathrm{Fix}(H) = \{b \in E | \sigma(b) = b$ 对所有 $\sigma \in H\}$, 则 $\mathrm{Fix}(H)$ 是 E/F 的一个中间域, 称为 H 的固定子域 (fixed field).

例 6.4.4 设 $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ 有理数 $\mathbf{Q}$ 上的扩张, 容易知道 $\mathbf{Q}(\sqrt{3}, \sqrt{5})/\mathbf{Q}$ 的 Galois 群中有同构

$$\sigma : \sqrt{3} \mapsto -\sqrt{3}, \quad \sqrt{5} \mapsto \sqrt{5}.$$

若 $H = \{e, \sigma\}$, 则 H 是 $\mathrm{Aut}\ \mathbf{Q}(\sqrt{3}, \sqrt{5})$ 的一个子群, 并且 H 的固定子域 $\mathrm{Fix}(H) = \mathbf{Q}(\sqrt{5})$. ■

不难证明, 下面结论成立.

性质 6.4.2 设 K_1, K_2 是 E/F 的中间域, $K_1 \subseteq K_2$, 则 $\mathrm{Gal}(E/K_1) \supseteq \mathrm{Gal}(E/K_2)$.

性质 6.4.3　设 H_1, H_2 是 $\mathrm{Gal}(E/F)$ 的子群, $H_1 \subseteq H_2$, 则 $\mathrm{Fix}(H_1) \supseteq \mathrm{Fix}(H_2)$.

性质 6.4.4　对 E/F 的任意中间域 K 都有 $K \subseteq \mathrm{Fix}(\mathrm{Gal}(E/K))$.

性质 6.4.5　对 $\mathrm{Gal}(E/F)$ 的任意子群 H 都有 $H \subseteq \mathrm{Gal}(E/\mathrm{Fix}(H))$.

3　Galois 群的阶

对于多项式的 Galois 群来说, 群 $\mathrm{Gal}(E/F)$ 的阶恰巧就是扩域的次数 $[E:F]$.

定理 6.4.1　设 $f(x) \in F[x]$ 在 F 上的分裂域是 E, 则

$$|\mathrm{Gal}(E/F)| = [E:F]$$

定义 6.4.4　设 E/F 是一个有限扩张, 若 $[E:F] = |\mathrm{Gal}(E/F)|$, 则称 E/F 为 Galois 扩张.

例 6.4.5　试证明扩张 $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ 不是 Galois 扩张.

证明　设 $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})$, $\alpha = \sigma(\sqrt[3]{2})$. 由于 $(\sqrt[3]{2})^3 = 2$, 故

$$\alpha^3 = \sigma(\sqrt[3]{2})^3 = \sigma((\sqrt[3]{2})^3) = \sigma(2) = 2.$$

但 $\sqrt[3]{2}$ 是 $\mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{R}$ 中唯一满足这个条件的数, 因此 $\alpha = \sqrt[3]{2}$, 从而 σ 是恒等映射, 因而 $|\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})| = 1 \neq [\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}]$, 所以扩张 $\mathbf{Q}[\sqrt[3]{2}]/\mathbf{Q}$ 不是 Galois 扩张. ■

定理 6.4.2　有限域的任何一个有限扩张是 Galois 扩张, 且 Galois 群是一个循环群.

证明　设 $F = F_q$ 是含 q 个元素的有限域, E 是 F 的一个 n 次有限扩张, 则 $E \cong F_{q^n}$. 令

$$\varphi : E \to E, \quad a \mapsto a^q.$$

则 $\varphi \in \mathrm{Gal}(E/F)$ 且 φ 生成 $\mathrm{Gal}(E/F)$ 的 n 阶循环子群.

因此 $|\mathrm{Gal}(E/F)| = n = [E:F]$, 所以 E/F 是 Galois 扩张, 并且 $\mathrm{Gal}(E/F)$ 是一个 n 阶循环群. ■

设 F 是域, $f(x)$ 是 $F[x]$ 中的非常数多项式, 若 $f(x)$ 是不可约的, 并且 $f(x)$ 在 F 的任意一个扩域中都没有重根, 则称 $f(x)$ 是可分的 (separable). 可以证明, 下面结论成立.

定理 6.4.3 有限扩张 E/F 是 Galois 扩张的充要条件为 E 是系数在 F 的某个可分多项式的分裂域.

Galois 基本定理指出：在域的 Galois 扩张的所有中间域和该域的 Galois 群的子群之间存在一一对应, 这样就可将域的扩张的问题转化为群论的问题来考虑.

定理 6.4.4 (Galois 理论基本定理) 若 E 是 F 的有限维 Galois 扩张, 则在该扩张的全部中间域所构成的集合与 Galois 群 $\mathrm{Gal}(E/F)$ 的全部子群所构成的集合之间存在一一对应, 并且

(1) 两个中间域的相对维数等于对应子群的相对指数. 特别地, $|\mathrm{Gal}(E/F)| = [E:F]$.

(2) F 在每个中间域 K 上都是 Galois 扩张, 另外, E 在 K 上是 Galois 扩张的充要条件是对应的子群 $\mathrm{Gal}(E/K)$ 是 $\mathrm{Gal}(E/F)$ 的正规子群, 并且此时,

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \text{ 与 } \mathrm{Gal}(K/F) \text{ 同构.}$$

若 K_1, K_2 是 E/F 的中间域, $K_1 \subseteq K_2$, 则定理中的相对维数是指维数 $[K_2 : K_1]$. 对于 Galois 的 H_1, H_2 是 $\mathrm{Gal}(E/F)$ 的子群, $H_1 \subseteq H_2$, 则将指数 $[H_2 : H_1]$ 称为 H_2 和 H_1 的相对维数.

Galois 基本定理是 Galois 理论的核心, 很多人都给出了不同的证明方法, 如 DeMeyer[①]等.

4 n 次多项式的 Galois 群

思考题 6.4.1 什么样的 n 次多项式, 它的 Galois 群刚好是 n 次对称群 S_n 呢?

下面来看看一般代数方程

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

这里 $a_n, a_{n-1}, \cdots, a_1, a_0$ 不是固定的数, 而是取任意变元.

既然系数是变元, 那么一般代数可写作

$$f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^{-i}\sigma_i x^{n-i} + \cdots + (-1)^n \sigma_n.$$

① DeMeyer F. Another proof of the fundamental theorem of Galois theory. Amer. Math. Monthly, 1968, 75: 720–724.

设 $x_1, x_2, \cdots, x_n$ 是 $f(x)$ 的 n 个根, 则由 $f(x) = (x - x_1)(x - x_2)\cdots(x - x_n)$ 可知

$$\sigma_1 = x_1 + \cdots + x_n,$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n,$$

$$\cdots$$

$$\sigma_n = x_1x_2\cdots x_n.$$

容易知道 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 为**初等对称多项式**, 并且 $f(x)$ 可以看做域 $\mathbf{Q}(\sigma_1, \sigma_2, \cdots, \sigma_n)$ 上的多项式, 可以证明下面结论成立.

定理 6.4.5　*n 次一般多项式的 Galois 群与对称群 S_n 的同构.*

当 $n \geqslant 5$ 时, S_n 不是可解群, 因此次数高于 4 的一般多项式的 Galois 群不是可解群.

思考题 6.4.2　*能用根式求解的方程的求根公式有些什么特点呢?*

例 6.4.6　$f(x) = x^2 + x - 1$ 可用根式求解 $x = \dfrac{-1 \pm \sqrt{5}}{2}$, 因此只要在有理数域 $\mathbf{Q}$ 上添加一个 $\sqrt{5}$, 就可得到 $\mathbf{Q}$ 的扩域 $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{5})$ 包含了 $x^2 + x - 1 = 0$ 的所有根, 此时, 显地有 $[\mathbf{Q}(\sqrt{5}) : \mathbf{Q}] = 2$.

一般地, 二次一般多项式 $f(x) = x^2 - bx + c$ 可看成 $F = \mathbf{Q}(b, c)$ 上的多项式. 只要将 $\sqrt{D} = \sqrt{b^2 - 4c}$ 添加到 F 上得到 F 的扩域 $F(\sqrt{D})$, 则 $F(\sqrt{D})$ 中包含了 $f(x)$ 的所有根 $x = \dfrac{b \pm \sqrt{D}}{2}$. 所以对于二次多项式 $f(x)$, 一定存在一个扩域 $F(\sqrt{D})/F$, 使得 $F(\sqrt{D})$ 包含 $f(x)$ 的所有根.

5　n 次多项式的根式求解

代数方程能否用根式求解可用根塔是否存在来刻画.

定义 6.4.5　*设 $f(x)$ 是某一首项系数为 1 的多项式, 系数都属于域 F, 称 $f(x) = 0$ 在 F 上可用根式求解, 如果存在 F 的某个扩域 K 满足以下条件:*

(1) *K 包含了 $f(x)$ 在 F 上的分裂域 E;*

(2) *扩域 K/F 有如下根塔*

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r \subseteq F_{r+1} = K.$$

其中每个 $F_{i+1}=F_i(d_i)$, $d_i^{n_i}=a_i\in F_i$, $i=1,2,\cdots,r$. 此时, 单扩张 $F_{i+1}=F_i(d_i)$ 称为根式扩张.

容易知道, 上面的定义与 $f(x)=0$ 的根可以通过有限次的加、减、乘、除和开方得到是等价的.

定理 6.4.6 设 F 为域, $F[x]$ 中多项式 $f(x)$ 在 F 上的 Galois 群为 G_f, 则 $f(x)=0$ 可用根式求解的充要条件为 G_f 是可解群.

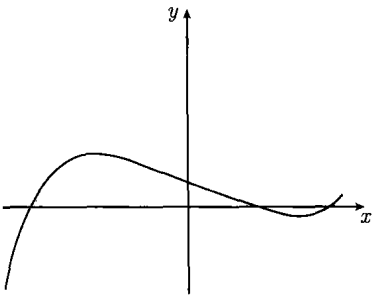
n 次一元多项式 $f(x)$ 的 Galois 群为 G_f 在 $n\geqslant 5$ 时不是可解群, 因此下面结论成立, 该结果是 Abel 在 19 岁时证明的.

定理 6.4.7 高于四次的一般代数方程不可能用根式求解.

不过, 对于特殊的代数方程, 如 $(x-1)^6=0$ 等是可以用根式求解的. 那么什么样的特殊代数方程可以用根式求解呢? Galois 解决了这个问题. 另外, 下面的漂亮结果也属于 Galois.

定理 6.4.8 设 $f(x)$ 是有理系数的素数 $p(p\geqslant 5)$ 次不可约多项式, 若 $f(x)$ 有且仅有一对共轭非实根, 则代数方程 $f(x)=0$ 不能用根式求解.

例 6.4.7 设 $f(x)=x^5-4x+2$, 则 $f(x)$ 的图形如右下图, $f(x)$ 有且仅有 3 个实根, 因此 $f(x)$ 仅有一对共轭非实根, 所以 $f(x)$ 不能用根式求解.



不过一般五次方程没有根式解并不等于它没有解, 只是它的解不能表为根式及简单的代数运算. 19 世纪 50 年代, Hermite, Kronecker 和 Brioschi 利用椭圆模函数分别得出一般五次方程的解析解. Klein 和 Gordan 还讨论过更高次方程的解.

Liouville 证明了一般的 Riccati 方程不可能用积分法积分①, 在 Liouville 之后, 微分方程的一个重要方向就是类似 Abel 和 Galois 的方法, 将群论和方程的可积性理论相联系. Picard 和 Vessiot 建立了微分 Galois 理论, 将群的可解性与方程的可积性密切联系起来. 由于线性常微分方程的解空间是有限维向量空间, 故方程的任意显式的解可用方程的任意一组显式的基础解线性表示, 从而可由方程系数所在的基本微分域通

① George Neville Watson. A treatise on the theory of Bessel functions, 2nd ed. Cambridge: Cambridge Univ Press, 1944: 111–123.

过有限次添加基础解中的特解, 使基本域扩张为方程的分裂域, 并引入分裂域上的微分自同构概念, 建立起微分方程的微分 Galois 群.

习　题　六

6.1　试求出 $\mathbf{Q}(\sqrt{3}+\sqrt{5})/\mathbf{Q}$ 的中间域.

6.2　试求出 $\mathbf{Q}(\pi)$.

6.3　设 K/F 为域的扩张, 若 $[K:F]$ 为素数, 试证明 $K=F(\alpha)$, 这里 α 是 K 中任意不属于 F 的元.

6.4　试求出 $\alpha=\sqrt{2}+\sqrt{3}$ 在 $\mathbf{Q}(\sqrt{6})$ 上的极小多项式.

6.5　试求出 $\alpha=\cos\dfrac{\pi}{9}+\mathrm{i}\sin\dfrac{\pi}{9}$ 在 $\mathbf{Q}$ 上的极小多项式.

6.6　设 α 是 F 上的代数元, 并且它的极小多项式为 $g(x)$, 若 $f(x)$ 是 F 上的多项式, 并且 $f(\alpha)=0$, 试证明 $g(x)$ 一定是 $f(x)$ 的因子.

6.7　设 F 是一个域, α 是 F 上的一个代数元, 若 $[F(\alpha):F]=5$, 试证明 $F(\alpha^2)=F(\alpha)$.

6.8　设 $f(x)=x^3+\overline{2}x+\overline{1}\in\mathbf{Z}_3[x]$, 试证明在域 $\mathbf{Z}_3[x]/(f(x))$ 中, $f(x)$ 一定有根.

6.9　试求多项式 $f(x)=(x^2+1)(x^2-2)$ 在有理数域 $\mathbf{Q}$ 上的分裂域.

6.10　若 p 为素数, 试求多项式 x^p-1 在 $\mathbf{Z}_p$ 上的分裂域.

6.11　试求 $\sqrt{2}+\sqrt{3}$ 在 $\mathbf{Q}$ 上的极小多项式.

6.12　设 $\alpha=\dfrac{-1+\sqrt{-3}}{2}$, 若 $F=\mathbf{Q}(\alpha)$, 试证明 $F(\sqrt[3]{2})/F$ 是 Galois 扩张.

6.13　试求多项式 x^3-2 在 $\mathbf{Q}$ 上的分裂域 E, 并求 $[E:\mathbf{Q}]$.

6.14　若 $f(x)=x^3+x^2+\overline{1}$ 是 $\mathbf{Z}_2$ 的多项式, 试求 $f(x)$ 在 F 上的 Galois 群.

6.15　求 $\mathbf{Z}_3$ 上多项式 $x^4+\overline{2}$ 的分裂域 E 和 Galois 群 $\mathrm{Gal}(E/\mathbf{Z}_3)$.

6.16　若 p 为素数, a 是 $\mathbf{Z}_p$ 上多项式 $f(x)=x^p-x-b$ 的根, 试证明 $\mathbf{Z}_p(a)$ 是 $\mathbf{Z}_p$ 的正规扩张.

6.17 求 Galois 群 $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})$.

6.18 若 a 和 b 可用尺规作出, 试用尺规作出 $\dfrac{a}{b}$.

6.19 试证明多项式 $f(x)=2x^5-5x^4+5$ 不能用根式求解.

6.20 试证明方程 $x^7-8x^3+3x^2=0$ 不能用根式求解.

6.21 试证明方程 $x^5-9x+3=0$ 不能用根式求解.

6.22 对于每个整数 $n\geqslant 5$, 有理数域 $\mathbf{Q}$ 上一定有某个 n 次方程 $f(x)$, 它最少有一个根不能用根式求解.

~~~~~~

诺特 (E. Noether) 1882 年 3 月 23 日生于德国 Erlangen, 1900 年入 Erlangen 大学, 1907 年在数学家 Paul Gordan 指导下获博士学位. 诺特的工作在代数拓扑学、代数数论、代数几何的发展中有重要影响. 1907–1919 年, 她主要研究代数不变式及微分不变式. 她在博士论文中给出三元四次型的不变式的完全组. 还解决了有理函数域的有限有理基的存在问题. 对有限群的不变式具有有限基给出一个构造性证明. 她不用消去法而用直接微分法生成微分不变式, 在格丁根大学的就职论文中, 讨论连续群 (Lie 群) 下不变式问题, 给出诺特定理, 把对称性、不变性和物理的守恒律联系在一起. 1920–1927 年间她主要研究交换代数与交换算术. 1916 年后, 她开始由古典代数学向抽象代数学过渡. 1920 年, 她已引入 “左模”、“右模” 的概念. 1921 年写出的《整环的理想理论》是交换代数发展的里程碑. 建立了交换诺特环理论, 证明了准素分解定理. 1926 年发表《代数数域及代数函数域的理想理论的抽象构造》, 给 Dedekind 环一个公理刻画, 指出素理想因子唯一分解定理的充分必要条件. 诺特的这套理论也就是现代数学中的 “环” 和 “理想” 的系统理论, 一般认为抽象代数形式的时间就是 1926 年, 从此代数学研究对象从研究代数方程根的计算与分布, 进入到研究数字、文字和更一般元素的代数运算规律和各种代数结构, 完成了古典代数到抽象代数的本质的转变. 诺特当之无愧地被人们誉为抽象代数的奠基人之一. 1927–1935 年, 诺特研究非交换代数与非交换算术. 她把表示理论、理想理论及模理论统一在所谓 “超复系” 即代数的基础上. 后又引进交叉积的概念并用决定有限维伽罗瓦扩张的布饶尔群. 最后导致代数的主定理的证明, 代数数域上的中心可除代数是循环代数.
~~~~~~

学习指导

本章重点

1. 域扩张的次数定理: 设 L 是 F 的有限扩域, K 是 L 的有限扩域, 则 $[K:F]=[K:L][L:F]$.

2. 对域 F 上任意次数大于零的多项式 $f(x)$, $f(x)$ 的分裂域不仅存在, 而且在同构下是唯一的.

3. 若实数 a 可用尺规作出, 则 a 必是有理数域 $\mathbf{Q}$ 上的代数元, 并且其极小多项式的次数等于 2 的幂.

4. 设 F 是任一域, $f(x)\in F[x]$, E 为 $f(x)$ 在 F 上的分裂域, G_f 为 $f(x)$ 在 F 上的 Galois 群, 则任意 $\sigma\in G_f$ 都将 $f(x)$ 的根映为 $f(x)$ 的根.

5. 设 F 为域, $F[x]$ 中多项式 $f(x)$ 在 F 上的 Galois 群为 G_f, 则 $f(x)=0$ 可用根式求解的充要条件为 G_f 是可解群.

6. 高于四次的一般代数方程不可能用根式求解.

释疑解难

1. 素域定义及其特征.

没有真子域的域称为素域. 由于域的特征不是素数就是 ∞, 故素域的特征也是素数或者 ∞. 从而在同构意义下, 素域只有两类: 一类是模 p (素数) 剩余类域 $\mathbf{Z}_p$, 特征为 p, 另一类是有理数域 $\mathbf{Q}$, 特征为 ∞.

2. 域同素子域的关系.

任何域 F 都包含且只包含一个素子域. 当域的特征为 p (素数) 时, 域 F 包含的素子域与 $\mathbf{Z}_p$ 同构, 当域的特征为 ∞ 时, 域 F 包含的素子域与有理数域 $\mathbf{Q}$ 同构.

3. 特征为 ∞ 的素域没有真子域, 但它可能会有很多真的子环. 这是由于整数环 $\mathbf{Z}$ 是有理数域 $\mathbf{Q}$ 的子环, 但 $\mathbf{Z}$ 有无限多个互不同构的子环, 特征为 ∞ 的素域都包含一个与 $\mathbf{Z}$ 同构的子环, 故特征为 ∞ 的素域一定有无穷多个子环. 不过特征为 p 的有限域 $\mathbf{Z}_p$ 只有平凡子环.

4. 极小多项式的性质：

(1) α 在域 F 上的极小多项式 $f(x)$ 在 F 上一定是不可约的.

(2) 若多项式 $g(x) \in F[x]$, $g(\alpha)=0$, $f(x)$ 为 α 在域 F 上的极小多项式, 则 $f(x)|g(x)$.

5. α 在域 F 上极小多项式是 n 次的, 则 F 的单扩张 $F(\alpha)$ 有如下的结构：

$$F(\alpha)=\{a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0|a_i\in F\},$$

并且 $F(\alpha)$ 是 F 上的 n 维向量空间.

6. 域 F 的超越元是不存在极小多项式的, 这是由于它不是 F 中任何非零多项式的根.

7. 如何判断一个元素是否为一个域上的代数元或超越元是一个相当困难的问题.

8. 若 F 为环, 则 $F[\alpha]$ 为包含 F 和 α 的最小的环. 容易验证

$$F[a]=\left\{\sum_{i=0}^{n}a_i\alpha^i|n\text{ 为某个正整数, }a_i\in F, i=1,2,\cdots,n\right\}.$$

(1) 设 E/F 是域扩张, $\alpha\in E$, 若 α 是 F 上的超越元, 则环 $F[\alpha]$ 与多项式环 $F[x]$ 同构, 并且域 F 的单扩张 $F(\alpha)$ 与多项式环 $F[x]$ 的分式域同构.

(2) 设 E/F 是域扩张, $\alpha\in E$, 若 α 是 F 上的代数元, 则环 $F[\alpha]$ 一定是域, 因而 $F[\alpha]$ 就是扩域 $F(\alpha)$.

9. 多项式 $f(x)$ 在不同域上的分裂域.

多项式 $f(x)$ 在不同域上的分裂域可能相同, 也可能不相同. 如 x^2-2 在有理数域 $\mathbf{Q}$ 上的分裂域与在 $\mathbf{Q}(\sqrt{2})$ 上的分裂域是相同的, 都是 $\mathbf{Q}(\sqrt{2})$.

10. 有限域子域的个数.

由于有限域 F 的阶一定是某个素数 p 的次幂 p^n, 故 F 的子域的阶必为 p^m, 并且 m 整除 n. 因此 n 的正因数个数就是 F 的子域的个数.

11. 若 F 是域, 则 Galois 群 $\mathrm{Gal}(F/F)$ 只含恒等同构一个元素. 另外, $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ 含有恒等同构和共轭同构两个元素.

12. 方程的 Galois 群的计算, 没有普遍性的方法.

13. 高于四次的一般代数方程没有根式解并不等于它没有解, 只是它的解不能表为根式及简单的代数运算.

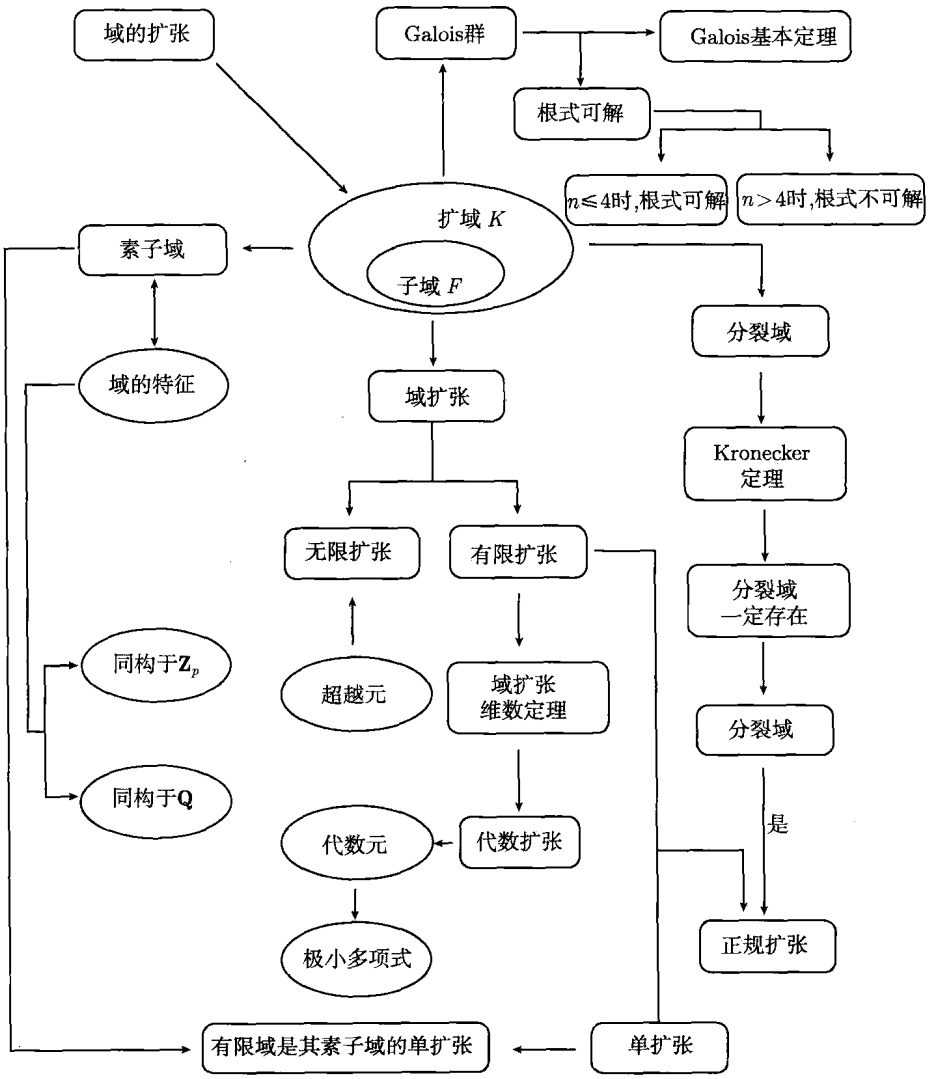
解题技巧

1. 构造 p^n 阶有限域的方法.

对于给定的素数 p 和一个正整数 n, 在域 $\mathbf{Z}_p$ 上取定一个 n 次不可约多项式 $f(x)$, 则域 $\mathbf{Z}_p$ 上的多项式环 $\mathbf{Z}_p[x]$ 的商环 $\mathbf{Z}_p[x]/(f(x))$ 就是一个 p^n 阶的有限域.

2. 设域 E 为域 F 的扩张, 掌握求 Galois 群 $\mathrm{Gal}(E/F)$ 的方法. 主要是要分析同构 σ 在保持 F 的元素不变时, 将形如扩域 $F(\alpha,\beta)$ 映为 $F(\alpha,\beta)$ 时, σ 可将 α 和 β 映为哪些元素, 从而确定 Galois 群的阶和结构.

知识点联系图


域的扩张
Galois群
Galois基本定理
根式可解
$n\leqslant 4$时,根式可解
$n>4$时,根式不可解
扩域 K
子域 F
素子域
域的特征
域扩张
分裂域
Kronecker
定理
无限扩张
有限扩张
分裂域
一定存在
同构于$\mathbf{Z}_p$
超越元
域扩张
维数定理
分裂域
同构于$\mathbf{Q}$
代数元
代数扩张
是
极小多项式
正规扩张
有限域是其素子域的单扩张
单扩张

第 7 章　群论在微分方程中的应用

大数学家, 如阿基米德、牛顿和高斯, 他们始终都是将理论与应用平等地结合成一个整体.

Klein (1849—1925, 德国数学家)

Abel 用群论的思想证明了五次和五次以上的多项式方程的解一般不可能用根式表达, Galois 给出了判断具体多项式的根可以用根式表达的条件, Liouville 证明了一般的 Riccati 方程不可能用初等积分法求其通解.Lie 建立了 Lie 群理论, 证明了对于给定的一阶常微分方程, 如果能找到一个该方程所接受的非平凡 Lie 群, 则该方程的解就可用积分形式表出.Picard 和 Vessiot 提出了微分 Galois 理论, 对线性微分方程建立了相应的微分 Galois 群, 证明了 n 次线性复系数方程一般不能用初等积分法求解, 从而将群的可解性与方程的可积性联系起来. 在这里, 将用最简单的方法, 介绍一下利用微分方程的不变群, 将常微分方程的求解问题转化为积分的方法.

7.1　微分方程的不变群

1　变换群

定义 7.1.1　设 $\mathbf{R}^n$ 是实数构成的 n 维向量空间, 即 $\mathbf{R}^n=\{(x_1,x_2,\cdots,x_n)|x_i\in\mathbf{R}\}$, 若 G 中的任一元素 g, 都可确定 $\mathbf{R}^n$ 上的一个变换 $g:\mathbf{R}^n\to\mathbf{R}^n$, 则称群 G 为作用于 $\mathbf{R}^n$ 上的一个变换群 (transformation group).

对于任意 $x\in\mathbf{R}^n$, 将 x 的像记为 gx. 不难看出, G 中的单位元确定了 $\mathbf{R}^n$ 上的恒等变换, g 的逆元 g^{-1} 确定的变换是变换 g 的逆变换.

例 7.1.1　$\mathbf{R}^2$ 上的旋转变换群是 $G=\{g_\theta|0\leqslant\theta<2\pi\}$, 对 θ 的加法 (对 2π 取模) 所成之群, 它在 $\mathbf{R}^2$ 上的作用规定为

$$g_\theta(x_1,x_2)=(y_1,y_2),$$

$$y_1 = x_1 \cos\theta - x_2 \sin\theta,$$

$$y_2 = x_1 \sin\theta + x_2 \cos\theta.$$

在研究变换群时, 最重要的是它的不变量.

定义 7.1.2 设 $F : \mathbf{R}^n \to \mathbf{R}$ 是一个实值函数, 并具有任意阶的导数, 若

$$F(gx) = F(x)$$

对任意的 $x \in \mathbf{R}^n$ 和 $g \in G$ 成立, 则称 F 为变换群 G 的一个不变量 (invariant).

例 7.1.2 对 $\mathbf{R}^2$ 上的变换群

$$G : \mathbf{R}^2 \to \mathbf{R}^2,$$

$$(x_1, x_2) \to (\lambda x_1, \lambda x_2), \quad \lambda > 0.$$

$F_1 = \dfrac{x_1}{x_2}$ 和 $F_2 = \dfrac{x_1 x_2}{x_1^2 + x_2^2}$ 都是它的不变量.

例 7.1.3 对 $\mathbf{R}^2$ 上的旋转变换群 G, $F = x_1^2 + x_2^2$ 是它的一个不变量, 实际上, 若 f 是任意阶可导的函数, 则 $f(x_1^2 + x_2^2)$ 都是 G 的不变量.

例 7.1.4 对 $\mathbf{R}^2$ 上的平移群 G:

$$G : \mathbf{R}^2 \to \mathbf{R}^2,$$

$$(x_1, x_2) \to (x_1 + c\varepsilon, x_2 + \varepsilon),$$

这里 c 为任意给定的常数, ε 是群 G 的参数, 则 $F = x_1 - cx_2$ 是它的一个不变量, 实际上, 若 f 是任意阶可导的函数, 则 $f(x_1 - cx_2)$ 都是 G 的不变量, 并且可以证明 G 的不变量一定具有形式 $f(x_1 - cx_2)$.

思考题 7.1.1 M 是群 G 的不变集是指对任意 $x \in M$ 和任意 $g \in G$, 有 $gx \in M$. 若 F 是任意阶可导的函数, $M = \{x | F(x) = 0\}$ 是群 G 的不变集, 则 F 是 G 的不变量吗?

不一定. 如 $G : \mathbf{R}^2 \to \mathbf{R}^2$, $(x_1, x_2) \to (\lambda x_1, \lambda x_2), \lambda > 0$, 容易知道

$$M = \{(x_1, x_2) | F(x_1, x_2) = 0\}, \quad \text{这里 } F(x_1, x_2) = x_1 x_2$$

是群 G 的不变集, 但 $F(x_1, x_2) = x_1 x_2$ 不是 G 的不变量.

不过, 若在上面的例子中, 要求对于任意 c, $M_c=\{(x_1,x_2)|F(x_1,x_2)=c\}$ 都是群 G 的不变集的话, 则 F 就一定是 G 的不变量.

性质 7.1.1　*设 G 是变换群, F 是任意阶可导的函数, 若对任意 $c, M_c=\{x|F(x)=c\}$ 都是群 G 的不变集, 则 F 一定是 G 的不变量.*

2　不变群

定义 7.1.3　*设 G 是 $\mathbf{R}^2$ 上的一个变换群, 若它使微分方程 $F=0$ 的解变为 $F=0$ 的解, 即当 $F(x,u)=0$ 时, 必有*

$$F(g(x,u))=0$$

对任意的 $g\in G$ 都成立, 则称 G 为微分方程 $F=0$ 的一个不变群.

对于最简单的一阶常微分方程 $\dfrac{\mathrm{d}u}{\mathrm{d}x}=f(x)$, 它的解是 $u=\displaystyle\int f(x)\mathrm{d}x$, 若取 G 为变换群 $G: x\mapsto x, u\mapsto u+c$, c 为任意常数, 则容易验证变换群 G 将方程的一个解映为方程的另一个解, 因此变换群 G 是微分方程 $\dfrac{\mathrm{d}u}{\mathrm{d}x}=f(x)$ 的一个不变群.

例 7.1.5　一阶常微分方程

$$\frac{\mathrm{d}u}{\mathrm{d}x}=u$$

有不变群.

证明　设 $u=u(x)$ 是上面方程的任一解, 则对于变换:

$$\varphi:(x,u)\to(y,v),$$

$$y=x+\varepsilon,$$

$$v=u.$$

故

$$\frac{\mathrm{d}v}{\mathrm{d}y}=\frac{\mathrm{d}u}{\mathrm{d}x}\frac{\mathrm{d}x}{\mathrm{d}y}=v.$$

所以 $v=v(y)$ 还是方程的解.

实际上, 由于方程 $\dfrac{\mathrm{d}u}{\mathrm{d}x}=u$ 的解为 $u=c\mathrm{e}^x$, 容易知道 $v=c\mathrm{e}^{y-\varepsilon}=c_1\mathrm{e}^y$ 还是方程的解.

例 7.1.6 一阶常微分方程

$$(u-x)\frac{\mathrm{d}u}{\mathrm{d}x}+u+x=0$$

有不变旋转群.

证明 设 $u=u(x)$ 是上面方程的任一解, 则对于任一旋转:

$$\theta:(x,u)\to(y,v),$$

$$y=x\cos\theta-u\sin\theta,$$

$$v=x\sin\theta+u\cos\theta.$$

故

$$x=y\cos\theta+v\sin\theta,$$

$$u=-y\sin\theta+v\cos\theta.$$

因此

$$\frac{\mathrm{d}v}{\mathrm{d}y}=\left(\sin\theta+\frac{\mathrm{d}u}{\mathrm{d}x}\cos\theta\right)\left(\cos\theta+\frac{\mathrm{d}v}{\mathrm{d}y}\sin\theta\right),$$

从而

$$(v-y)\frac{\mathrm{d}v}{\mathrm{d}y}+v+y=((u-x)\frac{\mathrm{d}u}{\mathrm{d}x}+u+x)\Big/\left(\cos\theta-\frac{\mathrm{d}u}{\mathrm{d}x}\sin\theta\right)=0.$$

所以 $v=v(y)$ 还是方程的解, 即旋转群是该微分方程的不变群.

例 7.1.7 二阶常微分方程

$$\frac{\mathrm{d}^2u}{\mathrm{d}x^2}=2u\frac{\mathrm{d}u}{\mathrm{d}x}.$$

不难验证

$$G_1:(x,u)\to(x+\varepsilon,u)$$

和

$$G_2:(x,u)\to(\lambda x,\lambda^{-1}u)$$

都是方程的不变群.

例 7.1.8 一阶常微分方程

$$\frac{\mathrm{d}u}{\mathrm{d}x}=xu^2-\frac{2u}{x}-\frac{1}{x^3},\quad x\neq 0.$$

不难验证

$$G_1:(x,u)\to(\mathrm{e}^{\varepsilon}x,\mathrm{e}^{-2\varepsilon}u)$$

是方程的不变群.

3　向量场

定义 7.1.4　设 $G=\{g_t|t\in\mathbf{R}\}$ 是作用于 $\mathbf{R}^n$ 上的一个单参数变换群, 对 $\mathbf{R}^n$ 的任意一点 x, g_t 作用在 x 的像就是 $\mathbf{R}^n$ 的一条曲线 $y=y(x,t)$, 称 $V=\left.\dfrac{\mathrm{d}y(x,t)}{\mathrm{d}t}\right|_{t=0}$ 为这个单参数变换群 G 的向量场 (vector field).

例 7.1.9　对于 $\mathbf{R}^2$ 上的旋转群 G, 由于

$$\frac{\mathrm{d}}{\mathrm{d}\theta}(x\cos\theta-y\sin\theta,x\sin\theta+y\cos\theta)|_{\theta=0}=(-y,x),$$

故 G 的向量场为 $V=-y\dfrac{\partial}{\partial x}+x\dfrac{\partial}{\partial y}$.

例 7.1.10　对于 $\mathbf{R}^2$ 上的平移变换群 G_ε, 由于

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}(x+c\varepsilon,y+\varepsilon)|_{\varepsilon=0}=(c,1),$$

故 G_ε 的向量场为 $V=c\dfrac{\partial}{\partial x}+\dfrac{\partial}{\partial y}$.

例 7.1.11　对于 $\mathbf{R}^2$ 上的相似变换群 G, 由于

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}(\mathrm{e}^\varepsilon x,\mathrm{e}^\varepsilon y)|_{\varepsilon=0}=(x,y),$$

故 G 的向量场为 $V=x\dfrac{\partial}{\partial x}+y\dfrac{\partial}{\partial y}$.

对于变换群 G, 怎么样才能求出 G 的不变量 F 呢?

例 7.1.12　对于 $\mathbf{R}^2$ 上的旋转群 G, 由于 G 的向量场为 $V=-y\dfrac{\partial}{\partial x}+x\dfrac{\partial}{\partial y}$, 故若考虑微分方程 $\dfrac{\mathrm{d}x}{-y}=\dfrac{\mathrm{d}y}{x}$, 则容易求出它的解为 $x^2+y^2=c$, 不难验证 $F(x,y)=x^2+y^2$ 就是 G 的不变量.

例 7.1.13　对于 $\mathbf{R}^2$ 上的相似变换群 G, 由于 G 的向量场为 $V=x\dfrac{\partial}{\partial x}+y\dfrac{\partial}{\partial y}$, 考虑微分方程 $\dfrac{\mathrm{d}x}{x}=\dfrac{\mathrm{d}y}{y}$, 则容易求出它的解为 $\dfrac{y}{x}=c,c\neq0$, 不难验证 $F(x,y)=\dfrac{y}{x}$ 就是 G 的不变量.

7.2 一阶常微分方程的求解

微分方程的不变群的一个应用就是一阶常微分方程的求解.

对于一阶常微分方程

$$\frac{\mathrm{d}u}{\mathrm{d}x} = F(x,u).$$

如果已知该方程的一个不变群

$$G : \mathbf{R}^2 \to \mathbf{R}^2,$$

它所对应的向量场为 V, 并且 $V(x_0,u_0) \neq 0$, 那么在 (x_0,u_0) 的附近可作坐标变换:

$$(x,u) \to (y,w);$$

$$y = \eta(x,u);$$

$$w = \zeta(x,u),$$

使得在坐标系 (y,w) 中, 向量场

$$V = \frac{\partial}{\partial w}$$

因而, 在坐标系 (y,w) 中, 方程不显含 w, 且 y 为 G 的一个不变量, 故原方程可化为

$$\frac{\mathrm{d}w}{\mathrm{d}y} = H(y).$$

解之, 得

$$w = \int H(y)\mathrm{d}y + c.$$

因此, 求解一阶常微分方程就转化为积分计算.

从上面的分析过程可知, 关键是如何寻找坐标变换, 由 $V = \dfrac{\partial}{\partial w}$ 可知, $\eta(x,u)$ 和 $\zeta(x,u)$ 应满足如下条件:

$$V \circ w = 1;$$

$$V \circ y = 0.$$

设 $V = \zeta(x,u)\dfrac{\partial}{\partial x} + \varphi(x,u)\dfrac{\partial}{\partial u}$, 则原方程可表示为

$$\zeta\frac{\partial w}{\partial x} + \varphi\frac{\partial w}{\partial u} = 1,$$

$$\zeta\frac{\partial y}{\partial x}+\varphi\frac{\partial y}{\partial u}=0.$$

因而, 求坐标变换就可转化为解上面的微分方程. 在不变群比较简单的情形, 就可以比较容易地找出它的不变量.

由于一阶齐次常微分方程

$$\frac{\mathrm{d}u}{\mathrm{d}x}=F\left(\frac{u}{x}\right)$$

有一个不变群 G

$$G:(x,u)\to(\mathrm{e}^{\varepsilon}x,\mathrm{e}^{\varepsilon}u),$$

由于

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}(\mathrm{e}^{\varepsilon}x,\mathrm{e}^{\varepsilon}u)|_{\varepsilon=0}=(x,u),$$

故 G 对应的向量场 $V=x\dfrac{\partial}{\partial x}+u\dfrac{\partial}{\partial u}$. 明显地, G 有不变量 $y=\dfrac{u}{x}$.

再由 $V\circ w=1$, 即方程 $x\dfrac{\partial w}{\partial x}+u\dfrac{\partial w}{\partial u}=1$ 可解得, $w=\ln x$ (或 $w=\ln u$), 因而可以作坐标变换

$$y=\frac{u}{x},$$
$$w=\ln x.$$

则

$$\begin{aligned}\frac{\mathrm{d}u}{\mathrm{d}x}&=\frac{\mathrm{d}(xy)}{\mathrm{d}x}=y+x\frac{\mathrm{d}y}{\mathrm{d}x}=y+x\frac{\mathrm{d}y}{\mathrm{d}w}\cdot\frac{\mathrm{d}w}{\mathrm{d}x}\\&=y+x\frac{\mathrm{d}y}{\mathrm{d}w}\cdot\frac{1}{x}=y+\frac{\mathrm{d}y}{\mathrm{d}w}.\end{aligned}$$

因此

$$y+\frac{\mathrm{d}y}{\mathrm{d}w}=F(y).$$

故原方程可化为

$$\frac{\mathrm{d}w}{\mathrm{d}y}=\frac{1}{F(y)-y}.$$

所以可以求出方程的解为

$$w=\int\frac{1}{F(y)-y}\mathrm{d}y+c.$$

例 7.2.1　对于一阶齐次常微分方程

$$\frac{\mathrm{d}u}{\mathrm{d}x}=\frac{u^2}{x^2}+\frac{u}{x},$$

有 $F(y)=y^2+y$, 作坐标变换

$$y=\frac{u}{x},$$

$$w=\ln x,$$

则原方程可化为

$$w=\int\frac{1}{y^2}\mathrm{d}y+c=-\frac{1}{y}+c.$$

故

$$\ln x=-\frac{1}{y}+c.$$

所以方程的解为

$$u=-\frac{x}{\ln x-c}.$$ ■

对于微分方程

$$(x-u\varphi(\sqrt{x^2+u^2}))\frac{\mathrm{d}u}{\mathrm{d}x}-x-u\varphi(\sqrt{x^2+u^2})=0,$$

容易验证旋转群是该方程的一个不变群.

由于

$$\frac{\mathrm{d}}{\mathrm{d}\theta}(x\cos\theta-u\sin\theta,x\sin\theta+u\cos\theta)|_{\theta=0}=(-u,x),$$

故 G 的向量场为 $V=-u\dfrac{\partial}{\partial x}+x\dfrac{\partial}{\partial u}$, 并且 G 有不变量 $r=\sqrt{x^2+u^2}$.

再由 $V\circ\theta=1$, 即方程 $-u\dfrac{\partial\theta}{\partial x}+x\dfrac{\partial\theta}{\partial u}=1$ 可解得, $\theta=\arctan\dfrac{u}{x}$, 因而可以利用坐标变换

$$x=r\cos\theta,$$

$$u=r\sin\theta$$

(这里 $r=\sqrt{x^2+u^2}$).

则可将原方程化为

$$\frac{\mathrm{d}\theta}{\mathrm{d}r}=\frac{\varphi(r)}{r},$$

解之, 得

$$\theta=\int\frac{\varphi(r)}{r}\mathrm{d}r+c,$$

这里 c 为任意常数.

例 7.2.2　对于一阶常微分方程 $\dfrac{\mathrm{d}u}{\mathrm{d}x}=\dfrac{x+u}{x-u}$, 由于 $\varphi=1$, 故它有解

$$\theta=\ln r+c.$$

所以它的解为 $2\arctan\dfrac{u}{x}=\ln(x^2+u^2)+C$.

7.3　常微分方程的降阶

面对一个二阶或更高阶的微分方程, 一般先降阶, 因为一个低阶的方程更容易分析和求解. 对高阶常微分方程, 可以通过坐标变换降阶.

二阶常微分方程

$$\frac{\mathrm{d}^2u}{\mathrm{d}x^2}+a(x)\frac{\mathrm{d}u}{\mathrm{d}x}+b(x)u=0$$

具有标度不变性, 则有不变群 G

$$G:(x,u)\to(x,\mathrm{e}^{\varepsilon}u)$$

(这里 ε 为群的参数), G 对应的向量场

$$V=u\frac{\partial}{\partial u}.$$

因此可以作坐标变换

$$y=x,$$

$$w=\ln u,$$

则

$$u=\mathrm{e}^w,$$

$$\frac{\mathrm{d}u}{\mathrm{d}x}=\frac{\mathrm{d}w}{\mathrm{d}y}\mathrm{e}^w,$$

$$\frac{\mathrm{d}^2u}{\mathrm{d}x^2}=\left[\frac{\mathrm{d}^2w}{\mathrm{d}y^2}+\left(\frac{\mathrm{d}w}{\mathrm{d}y}\right)^2\right]\mathrm{e}^w.$$

故原方程可化为

$$\frac{\mathrm{d}^2w}{\mathrm{d}y^2}+\left(\frac{\mathrm{d}w}{\mathrm{d}y}\right)^2+p(y)\frac{\mathrm{d}w}{\mathrm{d}y}+q(y)=0.$$

令 $z=\dfrac{\mathrm{d}w}{\mathrm{d}y}=\dfrac{1}{u}\dfrac{\mathrm{d}u}{\mathrm{d}y}$, 则原方程可化为 Riccati 方程

$$\frac{\mathrm{d}z}{\mathrm{d}y}+z^2+p(y)z+q(y)=0.$$

所以, 可以求出方程的解.

例 7.3.1 二阶常微分方程 $\frac{\mathrm{d}^2u}{\mathrm{d}x^2}-xu=0$, 由于它有不变群 G

$$G:(x,u)\to(x,\mathrm{e}^{\varepsilon}u),$$

G 对应的向量场

$$V=u\frac{\partial}{\partial u}.$$

故可以作坐标变换

$$y=x,$$

$$w=\ln u.$$

化简后, 有

$$\frac{\mathrm{d}^2w}{\mathrm{d}y^2}+\left(\frac{\mathrm{d}w}{\mathrm{d}y}\right)^2-y=0.$$

令 $z=\frac{\mathrm{d}w}{\mathrm{d}y}$, 则原方程可化为

$$\frac{\mathrm{d}z}{\mathrm{d}y}+z^2-y=0.$$

因此可求出方程的解.

~~~~~~

最后, 顺便指出, 群论在物理学和化学中也有很好的应用. 最早的应用之一是在晶体结构研究方面, 但这些并没有深奥的物理意义. 更重要的是 Wigner 在 20 世纪 20 年代末期发展了群论与量子力学之间的联系. 他最大的贡献是把群论应用于原子和原子核问题. 由于对原子核与基本粒子的研究, 特别是由于发现和应用基本对称性原理, 1963 年他与 Jenson 和 Mayer 一起获得诺贝尔物理奖. 目前, 群论已广泛应用于物理、化学、结晶学、生物等.

习 题 七

7.1 试证明变换 $u=x+\varepsilon, v=\frac{xy-\varepsilon}{x+\varepsilon}$ 构成一个单参数变换群.

7.2 对于微分方程 $(1-2x-\ln y)y'+2y=0$, 试求出 α 和 β, 使得

$$u=x+\alpha\varepsilon,\quad v=\mathrm{e}^{\beta\varepsilon}y$$
~~~~~~

为变换群, 并且保持方程的形式不变.

7.3　对于微分方程 $(x-y)^3y'=1$, 试求出 α 和 β, 使得

$$u=x+\alpha\varepsilon,\quad v=y+\beta\varepsilon$$

为变换群, 并且保持方程的形式不变.

~~~~~~

克罗内克 (L. Kronecker)1823 年 12 月 7 日生于德国布雷斯劳附近的利格尼茨 (现属波兰的莱格尼察), 1891 年 12 月 29 日卒于柏林. 他 1841 年入柏林大学, 1845 年获博士学位. 1861 年经库默尔推荐, 成为柏林科学院正式成员, 并以此身份在柏林大学授课. 1868 年当选为巴黎科学院通讯院士. 1880 年任著名的《克雷尔杂志》的主编. 1883 年接替库默尔成为柏林大学教授, 时年 60 岁. 1884 年成为伦敦皇家学会国外成员. 克罗内克最主要的功绩在于努力统一数论、代数学和分析学的研究. 他对代数和代数数论, 特别是椭圆函数理论有突出贡献. 克罗内克的数学观对后世有极大影响. 他主张分析学应奠基于算术, 而算术的基础是整数. 他的名言是: "上帝创造了整数, 其余都是人做的工作", 反映了其对当时的分析学持批判态度. 他作为直觉主义的代表人物, 还曾极力反对康托尔的集合论.

学习指导

本章重点

1. 单参数变换群.

2. 微分方程用变换群求解和降阶的方法.

释疑解难

1. 变换群中的变换不限于线性交换.

2. 在 $\mathbf{R}^2$ 上, 给出变换

$$y_1=f(x_1,x_2,\varepsilon),\quad y_2=g(x_1,x_2,\varepsilon)\quad(-\infty<\varepsilon<+\infty).$$

如果 (1) $\varepsilon=0$ 表示恒等变换, 即
~~~~~~

$$x_1 = f(x_1, x_2, 0), \quad x_2 = g(x_1, x_2, 0).$$

(2) $-\varepsilon$ 表示逆变换, 即

$$x_1 = f(y_1, y_2, -\varepsilon), \quad x_2 = g(y_1, y_2, -\varepsilon).$$

(3) 两个变换的 "乘积" 仍为变换, 若

$$z_1 = f(y_1, y_2, \delta), \quad z_2 = g(y_1, y_2, \delta).$$

两个变换的 "乘积" 为

$$z_1 = f(x_1, x_2, \varepsilon + \delta), \quad z_2 = g(x_1, x_2, \varepsilon + \delta).$$

则容易知道这些变换构成一个群, 称之为单参数变换群或 Lie 点变换群.

3. 常见的单参数变换群有:

(1) 平移群: $y_1 = x_1$, $y_2 = x_2 + \varepsilon$.

(2) 尺度变换群: $y_1 = \mathrm{e}^{\varepsilon} x_1$, $y_2 = \mathrm{e}^{\varepsilon} x_2$.

(3) 旋转群: $y_1 = x_1 \cos\varepsilon - x_2 \sin\varepsilon$, $y_2 = x_1 \sin\varepsilon + x_2 \cos\varepsilon$.

参 考 文 献

[1] 伯克霍夫, 麦克莱恩. 近世代数概论 (上). 北京: 人民教育出版社, 1979.

[2] Burn R P. Groups: a path to geometry. Cambridge University Press, 1987.

[3] 冯克勤. 近世代数三百题. 北京: 高等教育出版社, 2010.

[4] 韩士安, 林磊. 近世代数. 北京: 科学出版社, 2010.

[5] Hungerford T W. 代数学. 冯克勤译. 湖南: 湖南教育出版社, 1985.

[6] 克莱因. 古今数学思想 (第四册). 北京大学数学系数学史翻译组译. 上海: 上海科学技术出版社, 1981.

[7] Lam T Y. A first course in noncommutative rings, 2ed. GTM 131, Springer, 2001.

[8] 李翊神, 汪克林, 郭光灿, 汪秉宏. 非线性科学选讲. 合肥: 中国科学技术出版社, 1994.

[9] Olver P J. Applications of Lie groups to differential equations. New York: Springer-Verlag, 1993.

[10] 丘维声. 抽象代数基础. 北京: 高等教育出版社, 2003.

[11] Rotman J J. 抽象代数基础教程. 李样明, 冯明军译. 北京: 机械工业出版社, 2008.

[12] 腾加俊. 近世代数辅导与习题精解. 大连: 大连理工大学出版社, 2008.

[13] 田畴. 李群及其在微分方程中的应用. 北京: 科学出版社, 2005.

[14] V Sahai, V Bist. Algebra. 北京: 机械工业出版社, 2008.

[15] 谢邦杰. 抽象代数学. 上海: 上海科学技术出版社, 1982.

[16] 姚慕生. 抽象代数学. 上海: 复旦大学出版社, 2009.

[17] 杨劲根. 近世代数讲义. 北京: 科学出版社, 2009.

[18] 杨子胥. 近世代数习题解. 济南: 山东科学技术版社, 2003.

[19] 杨子胥. 近世代数学习辅导与习题选解. 北京: 高等教育出版社, 2004.

部分习题解答

只要一门科学分支充满大量的问题, 它就充满了生命力. 缺少问题意味着死亡或独立发展的终止. 正如人类的每种事业都为了达到某种最终目的一样, 数学研究需要问题. 问题的解决锻炼了研究者的力量, 通过解决问题, 他发现新方法及新观点并扩大他的眼界.

Hilbert (1862—1943, 德国数学家)

习 题 一

1.2 设 $G=\{f(t)|f(t)$ 为 $[0,1]$ 的严格单调递增的连续函数, 并且满足 $f(0)=0, f(1)=1\}$, 对于 $f,g\in G$, 定义乘法 $f\cdot g(t)=f(g(t))$, 试证明 G 是一个群.

证明 取 $e(t)=t$ 作为单位元, 容易验证 G 是一个群.

1.4 设 G 是非交换群, 试证明一定存在 $a\in G$, 使得 $a^2=e$ 不成立.

证明 反证法. 假设对于任意的 $a\in G$, 都有 $a^2=e$ 成立, 则 $a^{-1}=a$. 故对任意的 $a,b\in G$, 有 $ab=(ab)^{-1}=b^{-1}a^{-1}$, 但 $b^{-1}a^{-1}=ba$, 因此 $ab=ba$ 对任意的 $a,b\in G$ 都成立.

1.6 若群 G 是有限群, $a,b\in G$, 试证明 ab 和 ba 的阶是一样的. 另外, 此时 abc, bca 和 cab 的阶是一样的吗?

证明 若 ab 的阶是 n, 则 $(ab)^n=e$. 由于 $(ba)^n=a^{-1}(ab)^na=e$, 因此 ba 的阶一定小于等于 n. 同样可以证明 ab 的阶一定小于等于 ba 的阶, 因而 ba 的阶一定也是 n. 另外, 由 $abc=c^{-1}(cab)c=a(bca)a^{-1}$, 不难验证 abc, bca 和 cab 的阶是一样的.

1.8 若 H 是交换群 G 中所有的有限阶的元素, 试证明 H 是 G 的一个子群. 如果 G 是非交换群, 那么 H 还是不是 G 的一个子群?

证明 若 H 是交换群 G 中所有的有限阶的元素, 则由单位元 e 的阶是有限

阶可知 H 不是空集. 对于 $a,b\in H$, 若 a, b 的阶分别为 m, n, 则由 G 是交换群可知, ab 的阶为 m, n 的最小公倍数 $[m,n]$, 因此 $ab\in H$. 由于 a^{-1} 的阶与 a 的阶相同, 故 $a\in H$ 时, 一定有 $a^{-1}\in H$, 所以 H 是 G 的一个子群.

如果 G 是非交换群, 那么 H 不一定是 G 的一个子群. 如 G 为实数 2 阶满秩方阵全体在矩阵乘法下构成的群, 对于

$$a=\begin{bmatrix}1 & -1\\ 0 & -1\end{bmatrix},\quad b=\begin{bmatrix}1 & 1\\ 0 & -1\end{bmatrix}$$

都是 G 的 2 阶元, 但

$$ab=\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix},\quad (ab)^n=\begin{bmatrix}1 & 2n\\ 0 & 1\end{bmatrix}.$$

故 ab 的阶是无限的, 因此 H 对于乘法不是封闭的, 所以 H 不是 G 的一个子群.

1.10　试证明任意一个群 G 都不可能是它的两个真子群 H 和 K 的并集.

证明　反证法. 假设 H 和 K 是群 G 的两个真子群, 并且 $G=H\cup K$. 则一定存在 $a\notin H,b\notin K$, 由 $G=H\cup K$ 可知, 一定有 $a\in K,b\in H$. 由于 $ab\in G=H\cup K$, 故 $ab\in K$ 或 $ab\in H$. 如果 $ab\in K$, 那么由 $a\in K$ 可得 $a^{-1}\in K$, 因此 $b\in K$, 但这与前面的 $b\notin K$ 矛盾. 如果 $ab\in H$, 那么由 $b\in H$ 可得 $b^{-1}\in H$, 因此 $a\in H$, 但这也与前面的 $a\notin H$ 矛盾. 所以, 由反证法原理可知群 G 不可能是它的两个真子群 H 和 K 的并集.

1.12　试证明循环群 $G=\langle a\rangle$ 的子群 H 一定是循环群.

证明　如果 $H=\{e\}$, 那么明显地, H 是循环群. 若 $H\neq\{e\}$, 则由于 H 非空, 一定存在某个 $k\neq 0$, 使得 $a^k\in H$, 因而 $a^{-k}\in H$. 故总有某个正整数 $k\neq 0$, 使得 $a^k\in H$. 令 r 为所有 $a^k\in H$ 的 k 中最小的正整数, 则对于任意 $a^l\in H,l\geqslant 1$, 一定有 r 整除 l, 否则的话, 必有小于 r 的正整数 s, 使得 $l=kr+s$, 从而 $a^s\in H$, 但这与令 r 为所有 $a^k\in H$ 中最小的正整数矛盾, 所以 H 一定是循环群 $H=\langle a^r\rangle$.

1.14　设 G 是一个群, $a,b\in G$, 若 a 的阶为素数 p, 并且 $a\notin\langle b\rangle$, 试证明 $\langle a\rangle$ 与 $\langle b\rangle$ 的交一定是 $\{e\}$.

证明　若 $c\in\langle a\rangle\cap\langle b\rangle$, 并且 $c\neq e$, 则存在正整数 $1\leqslant k<p$, 使得 $c=a^k$. 由于 $\langle a\rangle$ 是 p 阶循环群, 故 a^k 是 $\langle a\rangle$ 的一个生成元. 另外, 由 $a^k\in\langle a\rangle\cap\langle b\rangle$ 可知 $\langle a^k\rangle\subset\langle b\rangle$, 因而根据 $a\in\langle a\rangle=\langle a^k\rangle$, 有 $a\in\langle b\rangle$, 矛盾. 所以 $\langle a\rangle$ 与 $\langle b\rangle$ 的交一定是 $\{e\}$.

1.16 设 G 是所有有理数上的 2×2 满秩矩阵全体在矩阵的相乘的乘法下构成的非交换群, 试找出阶为无限的 a 和阶为有限的 b, 使得 ab 的阶是有限的.

解 不难验证, 对于

$$a=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix},$$

有

$$a^n=\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}.$$

因此 a 的阶是无限的.

取 $b=\begin{bmatrix}1 & -1\\ 0 & -1\end{bmatrix}$, 则 $b^2=\begin{bmatrix}1 & -1\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & -1\\ 0 & -1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, 因此 b 的阶为 2. 并且

$$ab=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & -1\\ 0 & -1\end{bmatrix}=\begin{bmatrix}1 & -2\\ 0 & -1\end{bmatrix},$$

故

$$(ab)^2=\begin{bmatrix}1 & -2\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & -2\\ 0 & -1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}.$$

所以, a 的阶为无限和 b 的阶为有限, 并且 ab 的阶是有限的.

1.18 试给出一个群 G, 使得 G 可以写成它的 3 个真子群的并集.

证明 设

$$G=\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix},\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix},\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\right\}.$$

则 G 在矩阵乘法下是一个群.

明显地, G 有 3 个 2 阶子群

$$H_1=\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\right\},\quad H_2=\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\right\},$$

$$H_3=\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\right\}$$

并且 $G_1=H_1\cup H_2\cup H_3$.

1.20 若群 G 的阶是奇数, 试证明对于任意的 $a \in G$, 存在唯一的 $b \in G$, 使得 $a = b^2$.

证明 对于任意的 $a \in G$, 由于 $o(a)||G|$, 故 a 的阶一定是奇数, 若 a 的阶为 1, 则明显地存在唯一单位元 $e \in G$, 使得 $a = e^2$. 若 $o(a) = 2k+1, k \in N$, 则 $a^{2k+1} = e$, 从而 $a = a^{-2k} = (a^{-k})^2$, 令 $b = a^{-k}$, 则 $a = b^2$.

假设还存在 $c \in G$, 使得 $a = c^2$, 则 c 的阶一定是奇数, 故由 $2k+1 = o(c^2)$ 可知 $o(c) = 2k+1$. 类似可证, $o(b) = 2k+1$, 因而

$$a^k = c^{2k} = c^{-1}, \quad a^k = b^{2k} = b^{-1},$$

所以由 $b^{-1} = c^{-1}$ 可得 $b = c$.

1.22 设

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}; \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 1 & 5 & 2 & 3 & 7 \end{pmatrix};$$

(1) 求 σ_1^{-1}, σ_1^{-1} 的阶;

(2) 求 $\sigma_2\sigma_1\sigma_2^{-1}$.

解 (1) 由于 $\sigma_1 = (15)(27)(364)$, $\sigma_2 = (163)(245)$, 故 $\sigma_1^{-1} = (463)(72)(51)$. 由 (463), (72) 和 (51) 是 2 循环可知, σ_1^{-1} 的阶是 6.

(2) $\sigma_2\sigma_1\sigma_2^{-1} = (62)(47)(135)$.

1.24 试给出 S_4 的一个正规子群.

证明 不难验证 $H = \{e, (12)(34), (13)(24), (14)(23)\}$ 是 S_4 的一个正规子群.

1.26 设 H 和 K 分别是群 G 的 m 与 n 阶子群, 若 m 与 n 互素, 试证明 $H \cap K = \{e\}$.

证明 容易验证 $e \in H \cap K$, 并且 $H \cap K$ 是群 H 的子群, 也是群 K 的子群. 因此由 Lagrange 定理可知

$$|H \cap K||m, \quad |H \cap K||n.$$

因而由 m 与 n 互素可得, $|H \cap K| = 1$, 所以 $H \cap K = \{e\}$.

1.28 设 H, K 是 G 的子群, 并且 H 是 G 的正规子群, 试证明 HK 是 G 的子群.

证明 对于任意的 $a \in G$, 由于 H 是 G 的正规子群, 则 $aH = Ha$. 故对任意的 $h_1, h_2 \in H$, $k_1, k_2 \in K$, 存在 $h_2' \in H$, 使得 $k_1 h_2 = h_2' k_1$. 因而有

$$(h_1 k_1)(h_2 k_2) = (h_1 h_2' k_1) k_2 = (h_1 h_2')(k_1 k_2) \in HK.$$

类似可证, 对任意的 $h_1 \in H$, $k_1 \in K$, 有 $(h_1 k_1)^{-1} \in HK$, 所以 HK 是 G 的子群.

1.30 设 n 是奇数, G 是阶为 $2n$ 的有限 Abel 群, 试证明 G 最多只有一个二阶子群.

证明 反证法. 假设存在 $a, b \in G$, $H = \{e, a\}, K = \{e, b\}$ 是 G 两个不同的二阶子群. 则由 G 是 Abel 群可知, $HK = \{e, a, b, ab\}$ 是 G 的 4 阶子群, 故由 Lagrange 定理可知 4 一定整除 $|G|$, 从而 4 整除 $2n$, 但这与 n 是奇数矛盾. 所以由反证法原理可知 G 最多只有一个二阶子群.

1.32 试证明单群的同态像是单群或单位元群.

证明 设 G_2 是单群 G_1 的同态像, 则 $f : G_1 \to G_2$ 的核 $\mathrm{Ker}(f)$ 是 G_1 的正规子群. 由于 G_1 是单群, 故 $\mathrm{Ker}(f)$ 为 G_1 或单位元群. 如果 $\mathrm{Ker}(f) = G_1$, 那么 $\{e\} = G_1/\mathrm{Ker}(f) \cong G_2$, 因此 G_2 是单位元群. 如果 $\mathrm{Ker}(f) = \{e\}$, 那么 $G_1 = G_1/\mathrm{Ker}(f) \cong G_2$, 因此 G_2 是单群.

1.34 设群 G_1 和群 G_2 是阶分别为 m, $n (m > n)$ 的循环群, 试证明 n 整除 m 的充要条件为存在 $f : G_1 \to G_2$ 为群 G_1 到群 G_2 的满同态.

证明 设 $f : G_1 \to G_2$ 是群 G_1 到群 G_2 的满同态, 则由同态基本定理可知 G_2 与 $G_1/\mathrm{Ker}(f)$ 同构. 因此 $G_1/\mathrm{Ker}(f)$ 与 G_2 的阶都是 n. 由 Lagrange 定理可知 $[G_1 : \mathrm{Ker}(f)]|\mathrm{Ker}(f)| = |G_1|$, 所以 n 整除 m.

反过来, 若 n 整除 m, 设 $G_1 = \langle a \rangle$, $G_2 = \langle b \rangle$, 则定义 $f : G_1 \to G_2$ 为 $f : a^k \to b^k$, 不难验证设 $f : G_1 \to G_2$ 是群 G_1 到群 G_2 的满同态.

1.36 设 H 是群 G 的正规子群, $[G : H] = m, |H| = n$, 并且 m, n 是互素的, 试证明 H 是 G 唯一的阶为 n 的子群.

证明 设 K 是 G 另一个阶为 n 的子群, 则由于 H 是群 G 的正规子群, 故 HK 是群 G 包含 K 的子群. 记 $|HK/H|$ 为 k, 则由 HK/H 是 G/H 的子群和 G/H 的阶为 m 可知 k 整除 m. 再根据 $HK/H \cong K/H \cap K$ 可知 $K/H \cap K$ 的阶为 k, 但

K 的阶为 n, 因而 k 整除 n. 因为 m, n 是互素的, 因此 k 一定是 1, 即 $HK = H$, 所以 H 是 G 唯一的阶为 n 的子群.

1.38　设 G_1 和 G_2 是两个群, 试证明 $G_1 \times G_2 \cong G_2 \times G_1$.

证明　对任意 $a_1 \in G_1, a_2 \in G_2$, 定义

$$f : G_1 \times G_2 \to G_2 \times G_1,$$

$$(a_1, a_2) \mapsto (a_2, a_1).$$

则不难验证 f 为 $G_1 \times G_2$ 到 $G_2 \times G_1$ 的同构, 所以 $G_1 \times G_2 \cong G_2 \times G_1$.

1.40　试证明 S_3 的所有真子群都是交换群, 即 S_3 是内交换群.

证明　容易知道 S_3 的真子群的阶只可能为 1, 2, 3, 因此它的子群都是循环群, 所以它们都是交换群, 但 S_3 是非交换群, 所以 S_3 是内交换群.

习　题　二

2.2　设 a 是环 $\mathbf{R}$ 的幂零元, 即存在正整数 n 使得 $a^n = 0$, 试证明 $1 - a$ 是 R 的可逆元.

证明　由于存在正整数 n 使得 $a^n = 0$, 故

$$(1-a)(1+a+a^2+\cdots+a^{n-1}) = 1 - a^n = 1,$$

$$(1+a+a^2+\cdots+a^{n-1})(1-a) = 1 - a^n = 1.$$

因此 $1 - a$ 是可逆元, 并且

$$(1-a)^{-1} = 1 + a + a^2 + \cdots + a^{n-1}.$$

2.4　设 R 是一个环, a, b 为 R 中的两个元素, 若 $a + b = ab$ 并且 $1 - a$ 有逆元, 试证明 $ab = ba$.

证明　由于 $a + b = ab$, 故

$$1 = ab - (a+b) + 1 = (1-a)(1-b)$$

由 $1 - a$ 有逆元可知 $(1-a)^{-1} = 1 - b$, 因而 $(1-b)(1-a) = 1$, 故

$$1 = (1-b)(1-a) = ba - (a+b) + 1 = ba - ab + 1.$$

因此 $ba-ab=0$, 所以 $ab=ba$.

2.6 设 S 是 R 的子环, 若 S 有无穷多个不同的理想, 问 R 是否有无穷多个理想? 证明或给出例子.

解 例如整数环 $\mathbf{Z}$ 是有理数环 $\mathbf{Q}$ 的子环, 由于不同的素数 $p,(p)$ 都是 $\mathbf{Z}$ 的真理想, 故 $\mathbf{Z}$ 有无穷多个不同的理想, 但只有零理想和 $\mathbf{Q}$ 本身.

2.8 试求模 6 剩余类环 $\mathbf{Z}_6$ 的所有理想.

解 不难验证

$$I_1=\{\overline{0}\},\quad I_2=\mathbf{Z}_6,\quad I_3=\{\overline{0},\overline{2},\overline{4}\},\quad I_4=\{\overline{0},\overline{3}\}$$

就是 $\mathbf{Z}_6$ 的所有理想.

2.10 设 S,T 是环 R 中的理想, $ST=\left\{\sum_{i=1}^{n}a_ib_i\middle|a_i\in S,b_i\in T,\ n\text{ 为某个正整数}\right\}$, 问 $ST=S\cap T$ 是否一定成立.

解 不一定. 如在整数环 $\mathbf{Z}$ 中, 取两个不是互素的正整数 m,n, 令 $S=m\mathbf{Z}$, $T=n\mathbf{Z}$, 则容易验证 $ST=mn\mathbf{Z}$, 但 $S\cap T=[m,n]\mathbf{Z}$, 这里 $[m,n]$ 是 m,n 的最小公倍数, 所以 $ST=S\cap T$ 不一定成立.

2.12 设 R 是环, $I=\{ab-ba|a,b\in R\}$, 若 I 是左理想, 试证明 I 是 R 中的理想.

证明 对任意 $a,b,c\in R$, 由于 I 是左理想, 故 $RI=I$. 由 $bc-cb\in I$ 可知 $a(bc-cb)\in I$, 故

$$(ab-ba)c=a(bc-cb)+(ac)b-b(ac)\in I.$$

所以 I 是 R 中的理想.

2.14 设 R 是环, 若 R 只有 $\{0\}$ 和 R 本身是它的左理想, R 没有其他理想, 试证明 R 是可除环.

证明 对任意 $a\in R,a\neq 0$, 由于 Ra 是 R 的左理想, 并且 $Ra\neq\{0\}$, 但 R 只有 $\{0\}$ 和 R 本身是它的左理想, 故一定有 $Ra=R$. 因而存在 $b\in R$, 使得 $ba=1$. 又由于 $b\neq 0$, 故 Rb 也是 R 的左理想, 并且 $Rb\neq\{0\}$, 所以同样有 $Rb=R$, 从而存在 $c\in R$, 使得 $cb=1$. 由 $ba=1$ 和 $cb=1$ 可知 $c=c1=c(ba)=(cb)a=1a=a$, 故 $ba=ab=1$, 从而 a 是乘法可逆元, 所以 R 是可除环.

2.16 设 I_1 和 I_2 是环 $\mathbf{R}$ 的两个理想, 试证明 $I_1I_2 \subseteq I_1 \cap I_2$, 并举例说明 I_1I_2 可以真包含在 $I_1 \cap I_2$ 内.

证明 由于 I_1 和 I_2 是环 $\mathbf{R}$ 的两个理想, 因此 $I_1I_2 \subseteq I_2$, $I_1I_2 \subseteq I_1$, 因而 $I_1I_2 \subseteq I_1 \cap I_2$.

在整数环 $\mathbf{Z}$ 中, 令 $I_1 = (2) = \{2a|a \in \mathbf{Z}\}$ 和 $I_2 = (4) = \{4a|a \in \mathbf{Z}\}$ 是 $\mathbf{Z}$ 的两个理想, $I_1I_2 = (8) = \{8a|a \in \mathbf{Z}\}$, 并且 $I_1 \cap I_2 = (4) = \{4a|a \in \mathbf{Z}\}$, 因此 I_1I_2 可以真包含在 $I_1 \cap I_2$ 内.

2.18 试找出 $\mathbf{Z}$ 到自身的一切同态映射, 并求出每一同态的核.

解 设 φ 是 $\mathbf{Z}$ 到自身的任意同态, 则对任意 $n \in \mathbf{Z}$, 有 $\varphi(n) = n\varphi(1)$, 且 $\varphi(1) = \varphi(1)\varphi(1)$, 因此 $\varphi(1) = 0$ 或 1.

若 $\varphi(1) = 0$, 则 $\varphi(n) = n\varphi(1) = 0$, 故 φ 是零同态, 它的核为 $\mathbf{Z}$.

若 $\varphi(1) = 1$, 则 $\varphi(n) = n\varphi(1) = n$, 故 φ 是恒等同态, 容易知道它的核为 $\{0\}$.

所以, $\mathbf{Z}$ 到自身的一切同态映射只有零同态或恒等同态两种, 它们的核分别为 $\mathbf{Z}$ 或 $\{0\}$.

2.20 试证明环 $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ 与环 $\mathbf{Z}_4$ 不是同构的.

证明 只需注意 $\mathbf{Z}_4$ 有一个非零元 $a = \overline{2}$, 使得 $a^2 = \overline{0}$, 但 $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ 没有这样的元素, 所以环 $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ 与环 $\mathbf{Z}_4$ 不是同构的.

2.22 设 R_1 和 R_2 是环, $f : R_1 \to R_2$, 对于任意 $a, b \in R_1$, 有 $f(a+b) = f(a) + f(b)$, 试证明 $f(a-b) = f(a) - f(b)$ 对任意 $a, b \in R_1$ 都成立.

证明 由于 $f(0+0) = f(0) + f(0)$, 故 $f(0) = 0$, 因此 $0 = f(a + (-a)) = f(a) + f(-a)$, 从而 $f(-a) = -f(a)$, 所以 $f(a-b) = f(a) - f(b)$.

2.24 试证明有理数域 $\mathbf{Q}$ 的自同构只有恒等同构.

证明 对于有理数域 $\mathbf{Q}$ 的自同构 f, 由于 $f(1) = 1$, 故 $f(m) = m, f\left(\frac{1}{n}\right) = \frac{1}{n}$, 从而

$$f\left(\frac{m}{n}\right) = f\left(m \cdot \frac{1}{n}\right) = f(m)f\left(\frac{1}{n}\right) = \frac{m}{n}.$$

所以 f 为恒等同构.

2.26 设 R 是交换整环, m 和 n 为互素的正整数, $a, b \in R$, 若 $a^m = b^m, a^n = b^n$, 试证明 $a = b$.

证明 若 $a = 0$ 或 $b = 0$, 则容易知道 $a = b$. 设 $a \neq 0, b \neq 0$, 由于 m 和 n 为互素, 因此存在整数 s 和 t, 使得 $sm + tn = 1$. 如果 $s \geqslant 0$, 那么必有 $t \leqslant 0$, 故

$$bb^{sm} = ba^{sm} = ba^{1-tn} = ab(a^n)^{-t} = ab(b^n)^{-t} = ab^{sm}.$$

从而 $a = b$. 如果 $s \leqslant 0$, 同理可证, 所以 $a = b$.

2.28 在整数环 $\mathbf{Z}$ 中, 若 p 为素数, 问 (p^2) 和 $(2p)$ 是不是素理想.

解 由于 $p^2 = p \cdot p \in (p^2)$, 但 $p \notin (p^2)$, 故 (p^2) 不是素理想. 类似地, $(2p)$ 也不是素理想.

2.30 任意环 R 都存在拓扑 τ, 使得 R 成为拓扑环吗?

解 在任意给定的环 R 上, 定义 τ 为离散拓扑, 容易验证, 环 R 在离散拓扑 τ 下是拓扑环.

习 题 三

3.2 在 $\mathbf{Z}_3[x]$, 设 $f(x) = \overline{2}x^4 + \overline{2}x + \overline{1}, g(x) = x^2 + x + \overline{2}$, 试求出 $g(x)$ 除 $f(x)$ 的商和余式.

解 由于

$$\begin{aligned} f(x) &= \overline{2}x^4 + \overline{2}x + \overline{1} \\ &= \overline{2}x^2 g(x) + x^3 + \overline{2}x^2 + \overline{2}x + \overline{1} \\ &= \overline{2}x^2 g(x) + xg(x) + x^2 + \overline{1} \\ &= \overline{2}x^2 g(x) + xg(x) + g(x) + \overline{2}x + \overline{2}, \end{aligned}$$

则

$$f(x) = (\overline{2}x^2 + x + \overline{1})g(x) + \overline{2}x + \overline{2}.$$

3.4 设 F 为域, $a_1, a_2, \cdots, a_n$ 为 F 中 n 个不同的元素, 试证明存在域 F 上的多项式 $f(x)$, 使得对 $a_i \in F$, 有 $f(a_i) = 1$ 对任意 i 成立.

证明 取

$$g_i(x) = (x - a_1)(x - a_2) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n).$$

则 $g_i(a_i) \neq 0, g_i(a_j) = 0$ 对任意 $i \neq j$ 都成立. 令

$$f(x) = \sum_{i=1}^{n} g_i(a_i)^{-1} g_i(x),$$

则 $f(a_i) = 1$ 对任意 i 成立.

3.6 试给出例子说明环 $R[x]$ 中的 m 次与 n 次多项式的乘积可能不是一个 $m+n$ 次多项式.

解 在 $\mathbf{Z}_6[x]$ 中, 令

$$f(x) = \overline{3}x^3 + \overline{3}x^2, \quad g(x) = \overline{2}x^2 + 1.$$

则 $f(x)$ 为 3 次多项式, $g(x)$ 为 2 次多项式, 但

$$f(x)g(x) = \overline{3}x^3 + \overline{3}x^2$$

是 3 次多项式.

3.8 试求出 $\mathbf{Z}_3$ 上的所有首一 2 次不可约多项式.

解 由于 $\mathbf{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, 故 $\mathbf{Z}_3$ 上的 2 次多项式有如下的不可约多项式:

$$x^2 + \overline{1}, \quad x^2 + x + \overline{2}, \quad x^2 + \overline{2}x + \overline{2}.$$

3.10 试将 $x^9 - 1$ 在 $\mathbf{Z}[x]$ 中作素因子分解.

解 $x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

3.12 试证明 $f(x) = x^2 + 1 \in \mathbf{Z}[x]$ 是整数上的多项式环 $\mathbf{Z}[x]$ 上的不可约元.

证明 反证法. 假设 $x^2 + 1$ 在 $\mathbf{Z}[x]$ 中是可约的, 则存在一次多项式 $g(x) = ax + b$ 和 $h(x) = cx + d$, 使得 $f(x) = x^2 + 1 = g(x)h(x)$. 由于

$$(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd,$$

故 $ac = 1, ad + bc = 0, bd = 1$. 因此由 $a, c \in Z, ac = 1$ 可知 $a = c = \pm 1$, 同理可得 $b = d = \pm 1$. 但这与 $ad + bc = 0$ 矛盾, 因此 $x^2 + 1$ 在 $\mathbf{Z}[x]$ 中是不可约的.

3.14 设 R 是主理想交换整环, 试证明对任意 $a, b \in R$, a, b 都有最大公约元 d 存在, 并且有 $u, v \in R$, 使得 $d = ua + vb$.

证明 对于 $a,b\in R$, 由于理想 (a) 和理想 (b) 的和 $(a)+(b)$ 也是 R 的一个理想, R 是主理想整环, 故 $(a)+(b)$ 是 R 的一个主理想, 因此存在 $d\in R$, 使得 $(a)+(b)=(d)$.

由于 $a,b\in(a)+(b)$, 故 $a,b\in(d)$, 因此 $a|d$ 并且 $b|d$. 另外, 若 $c\in R$, $c|a$ 并且 $c|b$, 则 $a\in(c)$ 并且 $b\in(c)$, 故 $d\in(d)=(a)+(b)\subseteq(c)$, 因而 $c|d$, 所以 d 是最大公约元.

由 $d\in(d)=(a)+(b)$ 可知, $u,v\in R$, 使得 $d=ua+vb$.

3.16 设 R 是有理数域上的 2×2 阶矩阵构成的非交换环, 若 $f(x),g(x)\in R[x]$,

$$f(x)=\begin{bmatrix}2&1\\0&0\end{bmatrix}x^2+\begin{bmatrix}0&0\\1&0\end{bmatrix}x+\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad g(x)=\begin{bmatrix}0&1\\-1&0\end{bmatrix}x+\begin{bmatrix}1&1\\1&1\end{bmatrix}$$

试分别求出 $f(x)$ 被 $g(x)$ 右除所得到的右余式, 以及被 $g(x)$ 左除所得到的左余式.

证明 若 $f(x)=g(x)q_1(x)+r_1(x)$ 和 $f(x)=q_2(x)g(x)+r_2(x)$, 则容易知道 $q_1(x)$ 和 $q_2(x)$ 都是一次多项式, 故可设 $q_1(x)=a_1x+b_1$ 和 $r_1(x)=c_1$, $q_2(x)=a_2x+b_2$ 和 $r_2(x)=c_2$, 代入后比较系数可知

$$q_1(x)=\begin{bmatrix}0&0\\2&1\end{bmatrix}x+\begin{bmatrix}-1&1\\-2&-1\end{bmatrix},\quad r_1(x)=\begin{bmatrix}4&0\\3&1\end{bmatrix},$$

并且

$$q_2(x)=\begin{bmatrix}1&-2\\0&0\end{bmatrix}x+\begin{bmatrix}1&-1\\0&-1\end{bmatrix},\quad r_2(x)=\begin{bmatrix}1&0\\1&2\end{bmatrix}.$$

习 题 四

4.2 试证明 $V=\left\{\begin{bmatrix}a&a+b\\a+b&b\end{bmatrix}\middle|a,b\in\mathbf{Z}_5\right\}$ 是 $\mathbf{Z}_5$ 上的向量空间, 并求出 V 的一个基.

证明 只需定义容易验证 V 是 $\mathbf{Z}_5$ 上的向量空间, V 的一个基为

$$\left\{\begin{bmatrix}\bar1&\bar1\\\bar1&\bar0\end{bmatrix},\begin{bmatrix}\bar0&\bar1\\\bar1&\bar1\end{bmatrix}\right\}.$$

4.4 设 $\mathbf{Z}^2[x]$ 为 $\mathbf{Z}$ 上的次数小于等于 2 的多项式全体所构成的向量空间, 定义线性变换 $T:\mathbf{Z}^2[x]\to\mathbf{Z}^2[x]$, $T:f(x)\mapsto f'(x)-f(0)$, 试求出 T 的核空间 $\mathrm{Ker}(T)$ 和像空间 $\mathrm{Im}(T)$ 的一个基.

解 对于 $f(x)=a_2x^2+a_1x+a_0$, 有 $T(f(x))=2a_2x+a_1-a_0$, 故 $f(x)\in\mathrm{Ker}(T)$ 时, 有 $2a_2x+a_1-a_0=0$, 因此 $a_2=0, a_1=a_0$, 因而 $\mathrm{Ker}(T)=\{ax+a|a\in\mathbf{Z}\}$, 所以 $\{x+1\}$ 是 T 的核空间 $\mathrm{Ker}(T)$ 的一个基.

由于 $\{1,x,x^2\}$ 是 $\mathbf{Z}^2[x]$ 的一个基, 故 $\{T(1),T(x),T(x^2)\}$ 张成像空间 $\mathrm{Im}(T)$, 所以 $\mathrm{Im}(T)$ 有一个基为 $\{1,x\}$.

4.6 在 $\mathbf{Z}_{11}$ 上的多项式构成的向量空间 $\mathbf{Z}_{11}[x]$ 中, 对任意 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0\in\mathbf{Z}_{11}[x]$, 定义内积 $(f(x),g(x))=a_nb_n+a_{n-1}b_{n-1}+\cdots+a_1b_1+a_0b_0$(这里不妨设 $n\geqslant m$, 当 $i>m$ 时, 取 $b_i=0$). 令

$$W=\{a_3x^3+a_2x^2+a_1x+a_0|a_0,a_1,a_2,a_3\in\mathbf{Z}_{11}\},$$

试求 W 的正交补 $W^\perp$.

解 容易验证 $W^\perp=\{x^4f(x)|f(x)\in\mathbf{Z}_{11}[x]\}$.

4.8 整数加法群 $\mathbf{Z}_6$ 是交换环 $\mathbf{Z}_6$ 上的模, 试证明 $\overline{2}$ 和 $\overline{3}$ 是线性相关的.

证明 在环 $\mathbf{Z}_6$ 中, 取 $\overline{2},\overline{3}\in\mathbf{Z}_6$, 则 $\overline{2}\cdot\overline{3}+\overline{3}\cdot\overline{2}=0$, 所以按线性相关的定义, $\overline{2}$ 和 $\overline{3}$ 是线性相关的.

4.10 设 M 是交换环 R 的理想, 则 M 是交换环 R 上的模, 试证明任意非零元 $a,b\in M$, a 和 b 都是线性相关的.

证明 对任意 $a,b\in M$, 由于 $ba+(-a)b=0$, 故 a 和 b 都是线性相关的.

习 题 五

5.2 试求出 4 次交错群 A_4 的所有 Sylow 子群.

解 由于 $|A_4|=12=2^2\cdot3$, 故 A_4 有 4 阶 2-Sylow 子群和 3 阶的 3-Sylow 子群. Klein 四元群

$$K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$$

是 A_4 的一个 2-Sylow 子群. 可以验证, K_4 是 A_4 的正规子群, 因此 K_4 是 A_4 的唯一 2-Sylow 子群.

A_4 的所有 3- 循环生成的子群为 A_4 的全部 3-Sylow 子群, 有

$$\langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle.$$

5.4 若有限群 G 的阶为 35, 试证明 G 一定是循环群.

证明 由于 $35 = 5 \cdot 7$, 故 G 有 5-Sylow 子群和 7-Sylow 子群. 若用 H 和 K 分别记 G 的 5-Sylow 子群和 7-Sylow 子群, 则 $|H| = 5$, $|K| = 7$, 因此 H 和 K 都是循环群. 由于 5-Sylow 子群的个数被 5 除余数为 1, 故 5-Sylow 子群只有 1 个. 同样可知 7-Sylow 子群也只有 1 个. 因而它们都是 G 的正规子群. 又由于 $H \cap K = \{e\}$, 故对任意 $h \in H, k \in K$, 有 $hk = kh$. 设 $H = \langle a\rangle, K = \langle b\rangle$, 则 $HK = \langle ab\rangle$, 容易知道 $o(ab) = 35$, 所以 $G = \langle ab\rangle$ 是循环群.

5.6 设 G 是 168 阶的单群, 试确定 G 中所有阶为 7 的元素.

证明 由于 $168 = 2^3 \cdot 3 \cdot 7$, 故 G 有 7-Sylow 子群, 并且个数整除 24, 因此有 1 个或 8 个 7-Sylow 子群. 若只有唯一的 7-Sylow 子群, 则该 7-Sylow 子群是正规子群, 但这与 G 是单群矛盾, 故 G 一定有 8 个 7-Sylow 子群, 每个 7-Sylow 子群都是循环子群, 因而都有 6 个 7 阶元素, 所以群 G 一共有 48 个 7 阶元素.

5.8 试证明 196 阶群 G 一定有一个阶大于 1 的 Sylow 子群, 它是 G 的一个正规子群.

证明 事实上, 只需证明群 G 有唯一的阶大于 1 的 Sylow 子群, 由于

$$|G| = 196 = 2^2 \cdot 7^2.$$

设 H 是 G 的一个 7-Sylow 子群, 因此与 H 共轭的子群个数 $k = 7q + 1$ 应该是 196 的正因子, 因而只能是

$$1, 2, 4, 7, 28, 49, 98, 196.$$

从而 $q = 0$, 故 $k = 1$, 即 H 是群 G 唯一的 7-Sylow 子群, 所以 H 是 G 的一个正规子群.

5.10 试证明 200 阶群 G 有正规的 Sylow 子群.

证明 由于 $200 = 2^3 \cdot 5^2$, 5-Sylow 子群的个数为 $5k + 1$ 并且能整除 8, 故只能是 1, 因此 G 的 5-Sylow 子群是唯一的, 所以 G 有正规的 Sylow 子群.

5.12 设 G 是一个 p^3 阶非交换群 (这里 p 是素数), 试证明 $C(G)=G'$.

证明 由于 G 是一个非交换群, 故 $1<|C(G)|<p^3$. 若 $|C(G)|=p^2$, 则 $G/C(G)$ 一定是循环群, 但这与 G 是非交换群矛盾, 故 $|C(G)|=p$. 因而 $G/C(G)$ 是 p^2 阶的群, 因此 $G/C(G)$ 是交换群, 于是 $G'\subseteq C(G)$. 但 $G'\neq\{e\}$, 否则 G 就是交换群, 所以 $C(G)=G'$.

5.14 设 p,q 是不同素数, $p>q>1$, 试证明 p^2q 群 G 一定是可解群.

证明 设 n 是 G 的 p-Sylow 子群的个数, 根据 Sylow 定理可知, n 被 p 除余数为 1, 并且 n 整除 p^2q. 由于 $n=pk+1$, 故 $n+(-pk)=1$, 因此 p 和 n 互素, 从而 n 整除 q. 由 $p>q>1$ 可知 n=1, 因而 G 的 p-Sylow 子群只有一个 H, 从而 H 是 G 的非平凡正规子群, 故 G 有一个正规群列 $\{e\}\triangleleft H\triangleleft G$, 并且 G/H 是 Abel 群, 所以 G 一定是可解群.

习 题 六

6.2 试求出 $\mathbf{Q}(\pi)$.

解 容易验证 $\mathbf{Q}(\pi)=\left\{\dfrac{f(\pi)}{g(\pi)}\middle|f,g\text{ 为有理系数的多项式, 并且 }g\neq 0\right\}$.

6.4 试求出 $\alpha=\sqrt{2}+\sqrt{3}$ 在 $\mathbf{Q}(\sqrt{6})$ 上的极小多项式.

解 由于 $\alpha=\sqrt{2}+\sqrt{3}$ 是多项式 $f(x)=x^2-(5+2\sqrt{6})$ 的根, 并且 α 不属于 F, 故 α 在 $\mathbf{Q}(\sqrt{6})$ 上的极小多项式是 $x^2-(5+2\sqrt{6})$.

6.6 设 α 是 F 上的代数元, 并且它的极小多项式为 $g(x)$, 若 $f(x)$ 是 F 上的多项式, 并且 $f(\alpha)=0$, 试证明 $g(x)$ 一定是 $f(x)$ 的因子.

证明 由于一定有 $h(x),r(x)$, 使得 $f(x)=g(x)h(x)+r(x)$, 并且 $r(x)$ 的次数比 $g(x)$ 次数低, 故由 $f(\alpha)=0$ 和 $g(\alpha)=0$ 可知 $r(\alpha)=0$, 但 $r(x)$ 的次数比 $g(x)$ 次数低, $g(x)$ 为 α 的极小多项式, 因而 $r(x)=0$, 所以 $g(x)$ 一定是 $f(x)$ 的因子.

6.8 设 $f(x)=x^3+\overline{2}x+\overline{1}\in\mathbf{Z}_3[x]$, 试证明在域 $\mathbf{Z}_3[x]/(f(x))$ 中, $f(x)$ 一定有根.

证明 由于

$$\begin{aligned}[x+(f(x))]^3+\overline{2}[x+(f(x))]+\overline{1} &= x^3+(f(x))+\overline{2}x+(f(x))+\overline{1}\\ &= x^3+\overline{2}x+\overline{1}+(f(x))\\ &= (f(x)),\end{aligned}$$

故 $f(x)$ 在 $\mathbf{Z}_3[x]/(f(x))$ 中有根 $x+(f(x))$.

6.10 若 p 为素数, 试求多项式 $x^p-\overline{1}$ 在 $\mathbf{Z}_p$ 上的分裂域.

解 在 $\mathbf{Z}_p$ 上, 由于 $x^p-\overline{1}=(x-\overline{1})^p$, 故多项式 $x^p-\overline{1}$ 的分裂域为 $\mathbf{Z}_p$.

6.12 设 $\alpha=\dfrac{-1+\sqrt{-3}}{2}$, 若 $F=\mathbf{Q}(\alpha)$, 试证明 $F(\sqrt[3]{2})/F$ 是 Galois 扩张.

证明 由于 $\sqrt[3]{2}$ 在 F 上的极小多项式是 x^3-2, 并且在 $F(\sqrt[3]{2})$ 中可分解为

$$x^3-2=(x-\sqrt[3]{2})(x-\alpha\sqrt[3]{2})(x-\alpha^2\sqrt[3]{2}),$$

故 $F(\sqrt[3]{2})/F$ 是 Galois 扩张.

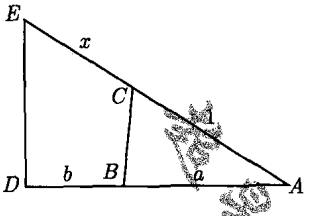
6.14 若 $f(x)=x^3+x^2+\overline{1}$ 是 $\mathbf{Z}_2$ 的多项式, 试求 $f(x)$ 在 F 上的 Galois 群.

证明 若 a 是 $f(x)$ 的一个根, 则 $a, a^2, a^2+a+\overline{1}$ 是 $f(x)$ 两两不同的根. 由 $f(\overline{0})=\overline{1}$ 和 $f(\overline{1})=\overline{1}$ 可知 $a\notin\mathbf{Z}_2$, 并且 $f(x)$ 在 $\mathbf{Z}_2$ 上是不可约的, 因此 $|G_f|=[\mathbf{Z}_2(a):\mathbf{Z}_2]=3$, 因为 S_3 的三阶子群是 A_3, 所以 $G_f=A_3$.

6.16 若 p 为素数, a 是 $\mathbf{Z}_p$ 上多项式 $f(x)=x^p-x-b$ 的根, 试证明 $\mathbf{Z}_p(a)$ 是 $\mathbf{Z}_p$ 的正规扩张.

证明 由于 a 是 $\mathbf{Z}_p$ 上多项式 $f(x)=x^p-x-b$ 的根, 故对任意 $d\in\mathbf{Z}_p$, 有 $(a+d)^p-(a+d)-b=(a^p-a-b)+(d^p-d)=0$, 因而 $f(x)$ 在 $\mathbf{Z}_p(a)$ 上有 p 个根, 所以 $\mathbf{Z}_p(a)$ 为多项式 $f(x)$ 在 $\mathbf{Z}_p$ 上的分裂域, 所以 $\mathbf{Z}_p(a)$ 是 $\mathbf{Z}_p$ 的正规扩张.

6.18 若 a 和 b 可用尺规作出, 试用尺规作出 $\dfrac{a}{b}$.



解 如果 a 和 b 是可用尺规作出的, 则用尺规可以作出右边的图, 容易知道三角形 ABC 和三角形 ADE 是相似的, 因此 $\dfrac{AB}{BD}=\dfrac{AC}{CE}$, 故 $\dfrac{a}{b}=\dfrac{1}{x}$, 因此 $x=\dfrac{a}{b}$, 从而 $\dfrac{a}{b}$ 是可用尺规作出的.

6.20 试证明方程 $x^7-8x^3+3x^2=0$ 不能用根式求解.

证明 由于方程 $x^5-8x+3=0$ 只有两个非实根, 并且它是不可约的, 故 $x^5-8x+3=0$ 不能用根式求解, 所以方程 $x^7-8x^3+3x^2=0$ 也有根是不能用根式求解的.

6.22 对于每个整数 $n\geqslant 5$, 有理数域 $\mathbf{Q}$ 上一定有某个 n 次方程 $f(x)$, 它最少有一个根不能用根式求解.

证明 由于多项式 $f(x)=2x^5-5x^4+5$ 在 $\mathbf{R}$ 中有三个根, 仅有一对共轭非实根, 所以 $f(x)=2x^5-5x^4+5$ 不能用根式求解.

若整数 $n\geqslant 5$, 令 $g(x)=x^{n-5}(2x^5-5x^4+5)$, 则容易知道 $g(x)$ 最少有一个根不能用根式求解.

习 题 七

7.2 对于微分方程 $(1-2x-\ln y)y'+2y=0$, 试求出 α 和 β, 使得

$$u=x+\alpha\varepsilon,\quad v=\mathrm{e}^{\beta\varepsilon}y$$

为变换群, 并且保持方程的形式不变.

解 将 $u=x+\alpha\varepsilon, v=\mathrm{e}^{\beta\varepsilon}y$ 代入方程 $(1-2u-\ln v)v'+2v=0$, 得

$$(1-2x-2\alpha\varepsilon-\ln(\mathrm{e}^{\beta\varepsilon}y))\mathrm{e}^{\beta\varepsilon}y'+2\mathrm{e}^{\beta\varepsilon}y=0,$$

即

$$(1-2x-2\alpha\varepsilon-\beta\varepsilon-\ln y)y'+2y=0.$$

故 $\alpha=1$ 和 $\beta=-2$ 时, $u=x+\varepsilon, v=\mathrm{e}^{-2\varepsilon}y$ 为变换群, 并且保持方程的形式不变.

索　引

A

Abel 群 (Abel group), 3

B

半群 (semigroup), 2
本原多项式 (primitive polynomial), 108
不可约元 (irreducible element), 101

C

超越元 (transcendental element), 173
初等对称多项式 (elementary symmetrical polynomial), 194
次数 (degree), 88

D

带余除法 (division with remainder), 92
代表元 (representative element), 22
代数闭域 (algebraically closed field), 177
代数扩张 (algebraic extension), 175
单扩张 (simple extension), 173
单群 (simple group), 29
第二同构定理 (second isomorphism theorem), 35
第一同构定理 (first isomorphism theorem), 35
多项式 (polynomial), 88

E

二元运算 (binary operator), 2

F

Fermat 小定理 (Fermat's little theorem), 20
分裂域 (splitting field), 179
分式域 (field of fractions), 70

G

Galois 扩张 (Galois extension), 192
Galois 群 (Galois group), 189
根 (root), 89
根式扩张 (radical extension), 195
共轭子群 (conjugate subgroup), 26
轨道 (orbit), 146

H

核 (kernel), 31
合成群列 (composition series of a group), 157
环 (ring), 53
换位子群 (commutator subgroup), 27

J

极大理想 (maximal ideal), 71
交错群 (alternating group), 14
交换环 (commutative ring), 53
阶 (order), 4

K

可解群 (solvable group), 160
可逆元 (invertible element), 3

L

Lagrange 定理 (Lagrange theorem), 19
理想 (ideal), 59
零因子 (zero divisor), 55
轮换 (cycle), 12

M

满同态 (surjective homomorppism), 31

N

内自同构 (inner automorphism), 32
逆元 (inverse element), 3

O

偶置换 (even permutation), 14

P

陪集 (coset), 16

Q

群 (group), 2
群的阶 (order of a group), 4
群作用 (group action), 144

S

商环 (quotient ring), 60
商群 (quotient group), 23
素理想 (prime ideal), 74
素域 (prime field), 169
Sylow 定理 (Sylow theorem), 153, 154
Sylow 子群 (Sylow subgroup), 152

T

特征 (characteristic), 72
拓扑群 (topological group), 41

W

无限群 (infinite group), 4

X

相伴 (associate), 101
像 (image), 31
循环群 (cyclic group), 8

Y

幺半群 (monoid), 2
有限群 (finite group), 4
有限域 (finite field), 178
有限扩张 (finite extension), 171
域 (field), 69

Z

正规化子群 (normalizer), 28
正规扩张 (normal extension), 185
正规子群 (normal subgroup), 22
中心 (center), 7
中心化子 (centralizer), 7
主理想 (principal ideal), 64
子环 (subring), 57
子群 (subgroup), 5
子域 (subfield), 69
自同构 (automorphism), 32
左陪集 (left coset), 16
左平移 (left translation), 145